KASPERSKY LAB

Kaspersky Anti-Virus® 5.5 for Linux, FreeBSD and OpenBSD Mail Servers

ADMINISTRATOR'S GUIDE

KASPERSKY ANTI-VIRUS® 5.5 FOR LINUX, FREEBSD AND OPENBSD MAIL SERVERS

アドミニストレータガイド

© Kaspersky Labs Japan
http://www.kaspersky.co.jp

目次

第 1 章 KASPERSKY ANTI-VIRUS 5.5 FOR LINUX, FREEBSD AND OPENBSD MAIL SERVERS 7
1.1. バージョン 5.5 における新機能 8
1.2. システム要件 9
1.3. マニュアルで使用されるシンボル 10

第 2 章 アプリケーションの一般的な導入方法 11
2.1. Kaspersky Anti-Virus の内部構造 11
2.2. メールシステムと同一サーバ上での運用 13
2.3. 2 次フィルタとしての運用 15
2.4. 専用サーバでの運用 16
2.5. 外部メールボックスから受信したメールのフィルタリング 18

第 3 章 KASPERSKY ANTI-VIRUS のインストール 21
3.1. Linux が稼働しているサーバへのインストール 21
3.2. FreeBSD または OpenBSD が稼働しているサーバへのインストール 22
3.3. インストール手順 22
3.4. アプリケーションの設定 23

第 4 章 インストール後の設定 25
4.1. アプリケーションのデフォルト設定 25
4.2. ウイルス定義データベースのインストール/更新 27
4.3. Webmin との連動設定 27
4.4. 手動でメールシステムと統合する 28
4.4.1. Sendmail との統合 28
4.4.2. Qmail との統合 29
4.4.3. Postfix との統合 30
4.4.4. Exim との統合 31
4.4.5. メールシステムと統合するための Kaspersky Anti-Virus の設定 32

第 5 章 KASPERSKY ANTI-VIRUS の使用 34
5.1. ウイルス定義データベースの更新 34
5.1.1. keepup2date アプリケーションコンポーネント 35
5.1.2. keepup2date コンポーネントの推奨設定 36
5.1.3. cron を使用したウイルス定義データベースの自動更新 37
5.1.4. ウイルス定義データベースの手動更新 38
5.1.5. ウイルス定義データベース用のネットワークディレクトリを作成する 39
5.2. サーバのメールトラフィックについてのウイルス保護 40
5.2.1. 感染していないメッセージおよび駆除済みメッセージの配信 40
5.2.2. 感染メッセージの配信 42
5.2.3. パスワードで保護されたアーカイブを含むメッセージの配信 43
5.2.4. 受信者へのメッセージ配信をブロックする 44
5.2.5. 添付ファイルの種類に基づくメッセージのフィルタリング 46
5.3. ファイルシステムのウイルス保護 48
5.3.1. オンデマンドスキャン 49
5.3.2. ディレクトリを毎日自動的にスキャンする(cron) 50
5.3.3. 高度なオプション：スクリプトファイルの使用 50
5.3.3.1. アーカイブ内の感染オブジェクトの駆除 50
5.3.3.2. 管理者への電子メール通知 51
5.3.4. 別のディレクトリにオブジェクトを移動する(隔離) 52
5.3.5. 処理対象オブジェクトのバックアップ 53
5.4. ライセンスキーの管理 54
5.4.1. ライセンスのメカニズム 54
5.4.2. ライセンスキー情報の表示 55
5.4.3. ライセンスの更新 57

第 6 章 高度な設定 58
6.1. メールトラフィックのウイルス保護の設定 58
6.1.1. ユーザグループの作成 60
6.1.2. メッセージのチェックおよび駆除モード 61
6.1.3. メールメッセージに関する動作 62

送信者、受信者、および管理者への通知 63
6.2. Postfix 用の追加機能 65
6.2.1. DSN 拡張のサポート 66
6.2.2. 8bit-MIME 拡張のサポート 66
6.2.3. X-Forward 拡張のサポート 67
6.2.4. 受信 SMTP のサポート 67
6.3. サーバファイルシステムのウイルス保護の設定 67
6.3.1. スキャン範囲 68
6.3.2. ファイルのスキャンおよび駆除モード 69
6.3.3. 感染の疑いがあるファイルおよび感染ファイルに適用する操作 70
6.3.4. バックアップモード 71
6.4. Kaspersky Anti-Virus の最適化 72
6.4.1. iChecker データベースの使用 72
6.4.2. サーバの負荷を軽減する 73
6.5. aveserver 処理の設定 73
6.5.1. aveserver のリロード 74
6.5.2. aveserver 処理の強制終了 74
6.6. 日付および時刻の表示形式を地域に合わせる 75
6.7. Kaspersky Anti-Virus のレポート用パラメータ 75
6.7.1. スキャンに関するメッセージの形式 77
6.7.2. コンソールに出力されるメッセージの形式 78
6.7.3. アプリケーションのウイルス統計情報 79
6.7.4. メッセージの追加データフィールド 80

第 7 章 KASPERSKY ANTI-VIRUS のアンインストール 81

第 8 章 KASPERSKY ANTI-VIRUS の動作検証 82

第 9 章 よくある質問（FAQ） 84

付録 A. カスペルスキーラブス 90
A.1. カスペルスキーラブスのその他の主な製品 90
A.2. お問い合わせ 92

付録 B. 使用許諾契約書 94

第1章 KASPERSKY ANTI-VIRUS 5.5 FOR LINUX, FREEBSD AND OPENBSD MAIL SERVERS

Kaspersky Anti-Virus® 5.5 for **Linux, FreeBSD, and OpenBSD Mail Servers**（以下 **Kaspersky Anti-Virus**）は、Linux, FreeBSD, OpenBSD 上で Sendmail, Postfix, Qmail, Exim を使用しているシステムにおけるメールトラフィックおよびファイルシステムのアンチウイルス機能を提供します。
Kaspersky Anti-Virus を使用して、以下のことが可能になります：

- 全マウントボリューム、SMTP トラフィックにおける送信メール・受信メールの *ウイルスチェック機能*。
- 感染ファイル・感染の疑いのあるファイル・破損ファイル・パスワードで保護されたファイル・ウイルススキャン不可能なファイルの *検知*。
- ファイルシステムおよびメールにおける感染コードの *除去*。
- ファイルシステムおよびメールトラフィックにおける感染ファイル・感染の疑いのあるファイル・破損ファイルの *隔離*。メールトラヒックにおいては、パスワードで保護されたファイルおよびスキャン不可能なファイルの隔離も可能。
- メール送信元（sender）とメール受信者（recipient）をグループ化し、あらかじめ設定されたルールに従いメールトラフィックを *制御*。
- ユーザ設定ルールに従い、添付ファイルのタイプや名前により *メールトラフィックを制御*。
- メールが感染している・感染の疑いがあるなどの場合、そのことを送信元（sender）・受信者（recipient）・システム管理者に *通知*。
- スケジュール機能もしくは手動でカスペルスキーのサーバからファイルをダウンロードすることにより、 *ウイルス定義データベースの更新*。

  ウイルス定義データベースは、感染コードの検索および除去に使用します。スキャン中は、ファイルのコードと定義ファイル内のコードを比較することによりウイルスの存在を分析します。ファイルがウイルスに感染している場合、データベース内に定義されている情報に従い、それを駆除します。

日々、新種のウイルスは出現します。従って、ウイルス定義データベースを最新に保つため、1 時間に一度のアップデートを推奨しています。

- ウェブベースのインターフェースを使用した*設定*。

1.1. バージョン 5.5 における新機能

- *keepup2date* がウイルス定義データベースやアプリケーションモジュールをダウンロードする際のトラフィックを新技術により低減しました。ダウンロード後のウイルス定義データベースの整合性チェック機能を搭載しました。
- 過去に駆除・削除した感染コードもしくはその疑いのあるコードを保存する機能を搭載しました。この機能により、駆除動作時にエラーが発生した際に元データを復旧させることが可能になりました。
- iChecker 機能とスキャン済みオブジェクトの二重キャッシュ機能により、ウイルススキャン時のサーバ負荷を軽減しました。
- webmin により、特定期間のウイルス検知数や検知したウイルス名の統計をリモートから確認できます。
- バックグランドにおける同時スキャンオブジェクト数を制限する機能を追加しました。これにより、サーバ負荷を最適化可能です。
- 検知可能なウイルスのリストを生成するようになりました。
- *smtpscanner* が使用するプロトコルとして、SMTP もしくは LMTP を選択可能になりました。
- SMTP 使用時にメール配送先の通知が可能になりました。
- 個々のメールについて、検知したウイルス名と *smtpscanner* が生成したレポートファイルの Message-ID の保存が可能になりました。
- Kaspersky Anti-Virus が使用する user を自動生成するようになりました。
- 使用するウイルス定義データベース（標準および拡張データベース）をユーザが設定できるようになりました。
- 通知時にに元メールのヘッダに挿入するマクロを増強しました。
- アプリケーションのインストール・アンインストール作業を簡素化しま

した。特に、アンインストール時に既存設定ファイルを適切に削除するようになりました。

- 古いバージョン（4.0 もしくは 5.0）の設定ファイルを移行することが可能になり、高速にインストールができるようになりました。
- インストーラは Kaspersky Anti-Spam を発見し統合します。また、アンインストール時に以前の設定を復元することが可能になりました。
- DSN, 8bit-MIME, 拡張 X-Forward, 着信転送を行う SMTP をサポートするようになりました。
- 既にスキャンされたメールのヘッダを更に Kaspersky Anti-Virus でスキャンした結果の情報付加機能を追加しました。

1.2. システム要件

Kaspersky Anti-Virus を使用する最小システム要件は以下です。

- ハードウェア必要条件：
  - Intel Pentium-class プロセッサ
  - 32 Mb 以上の RAM
  - 100 Mb 以上のディスクスペース
- ソフトウェア必要条件：
  - 以下のうちいずれかの OS
    - RedHat Linux versions 9.0, Fedora Core 3, Enterprise Linux Advanced Server 3,
    - SuSE Linux Enterprise Server 9.0 or Professional 9.2,
    - Mandrake Linux version 10.1
    - Debian GNU/Linux version 3.0 updated (r4)
    - FreeBSD versions 4.10 or 5.3
    - OpenBSD version 3.6
  - 次のうちいずれかのメール配送システム: Sendmail 8.x, Qmail 1.03, Postfix version snapshot_20000529 or higher, Exim 4.0
  - Kaspersky Anti-Virus の遠隔操作用に Webmin プログラム

(www.webmin.com)

- Kaspersky Anti-Virus インストールスクリプト（*install.sh*）用に Perl version 5.0 以上(www.perl.org)

1.3. マニュアルで使用されるシンボル

このマニュアルでは必要に応じて次の書体やシンボルが使用されています。それぞれの意味は下の表を参照してください。

形式	内容
太字	メニュータイトルやメニュー項目、ダイアログボックス名等を表します。
斜字体	ソフトウェアプログラムを示します。
情報	追加情報やコメント
注意	注意が必要な情報
実行 1. ステップ …	ユーザが実行する手順
タスク・例	タスクの設定、使用例
解決策	問題解決策
[key] – キー	コマンドラインキー
メッセージテキストとコマンドライン	コンフィグファイルやプログラムメッセージ、コマンドライン情報

第2章 アプリケーションの一般的な導入方法

Kaspersky Anti-Virus は、メールサーバの初期構造に応じて、以下のような導入方法を選択できます。

- *メールシステムと同一サーバ上に導入する。*サーバに Sendmail、Qmail、Postfix、Exim メールシステムがインストールされている場合に、この方法を使用します(13 ページのセクション 2.2 を参照)。
- *2 次フィルタとして専用サーバ上に導入する。*1 次メールサーバで、サポート対象外のオペレーティングシステムやメールシステムが稼働している場合に、この方法をお奨めします(16 ページのセクション 2.4 を参照)。
- *メールシステムと同一サーバ上に 2 次フィルタとして導入する。*メールサーバに Kaspersky Anti-Spam などのメールフィルタがインストールされている場合に、この方法をお奨めします(15 ページのセクション 2.3 を参照)。
- *外部メールボックス用のフィルタとして導入する。*メールサーバのユーザが外部サーバにメールボックスを持っていて、ダウンロードされるメールメッセージのウイルス保護を提供する場合に、この方法が役立ちます(18 ページのセクション **2.5** を参照)。

いずれの場合も、Kaspersky Anti-Virus は、メールトラフィックのフィルタと、実装されているすべてのファイルシステムのスキャンを行います。
上記の導入方法の詳細を説明する前に、Kaspersky Anti-Virus の運用アルゴリズムを完全に理解するために、Kaspersky Anti-Virus の内部構造について説明します。

2.1. Kaspersky Anti-Virus の内部構造

Kaspersky Anti-Virus を使用するにあたり、その運用アルゴリズムを理解する必要があります。
このセクションでは、このアプリケーションの内部構造について説明します。
サーバファイルシステムのスキャン処理は比較的わかりやすく、特別な学習を必要としないため、メールトラフィックスキャンを重点的に説明します。

Kaspersky Anti-Virus は、ウイルスメールのフィルタリングのみ行います。メールトラフィックの受信およびルーティングを行うメールエージェントとしての機能は備えていません。メールエージェントとしての機能は、サーバにインストールされているメールシステムが行います。アンチウイルスプログラムは、インストール後にメールシステムと統合されます。
以下の例では、メールシステムとの統合後のアプリケーションの内部動作を説明します。例として Sendmail メールシステムを使用します。

Sendmail システムにアンチウイルスが統合される際に、*sendmail.cf.listen* という追加設定ファイルが作成されます。
この設定ファイルを使用して起動された Sendmail は、受信したメールトラフィックをスキャンするために Kaspersky Anti-Virus に渡します。
元の設定ファイル*(sendmail.cf)*を使用して起動された場合は、アプリケーションから受信したメールメッセージを送信します。

運用アルゴリズムは以下の通りです(図 **1** を参照)。

1. Sendmail が SMTP プロトコル経由で送受信します(設定ファイルは *sendmail.cf.listen*)。Sendmail がキューを作成し、そこに受信メールを保存します。それらの受信メールをスキャンするために、LMTP または SMTP プロトコル経由で *smtpscanner* コンポーネントに渡します。
2. *smtpscanner* コンポーネントは、設定に従ってメールトラフィックを処理します。メールメッセージのスキャンおよび駆除は、以下のように行われます。
   a. *smtpscanner* が、ローカルソケットを使用して、メールメッセージのファイル名を *aveserver* コンポーネントに渡します。
   b. *aveserver* が、ウイルス定義データベースを使用して、オブジェクトのスキャンおよび駆除を行います。
   c. *smtpscanner* が、*aveserver* からファイルのステータスを定義するリターンコードを受け取ります。
   d. オブジェクトのステータスに応じて、*smtpscanner* が設定ファイルに従ってオブジェクトを処理します。
3. 処理が完了したメールトラフィックが、スキャンおよび駆除結果に関する通知と共に、SMTP プロトコル経由で Sendmail システムに送信されます(*sendmail.cf* 設定ファイルを使用)。Sendmail システムは、このメールトラフィックをローカルユーザに送信するか、他のメールサーバにルーティングします。

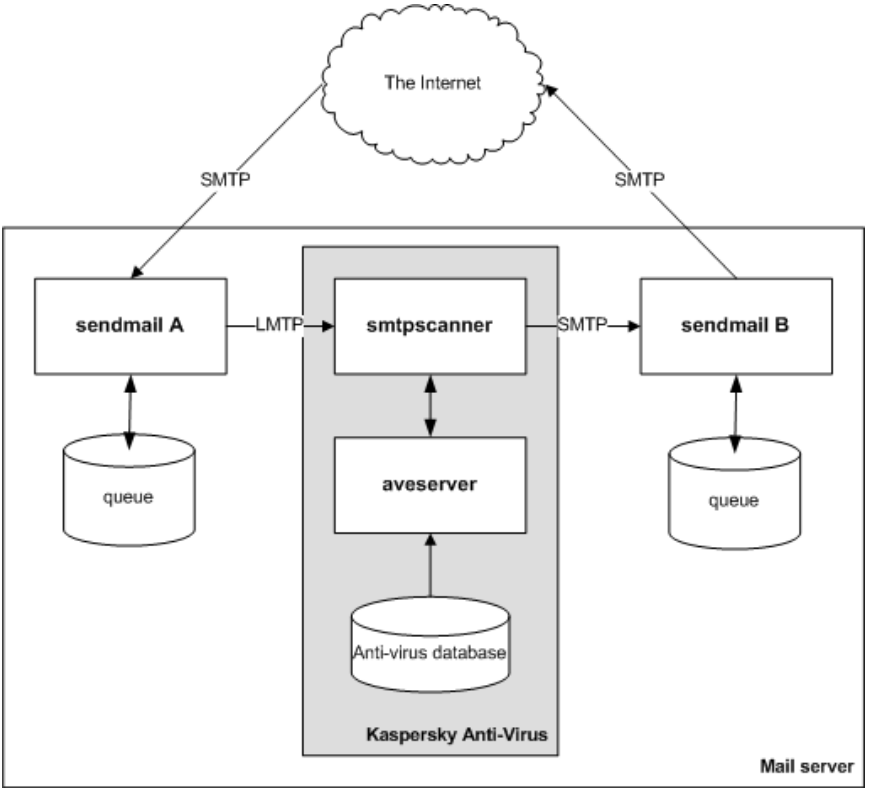

図 1. Kaspersky Anti-Virus for Unix Mail Servers の内部構造

2.2. メールシステムと同一サーバ上での運用

本書で説明されている Kaspersky Anti-Virus の運用および設定は、メールシステムがインストールされているサーバに Kaspersky Anti-Virus をインストールした場合のみを想定しています。

メールシステムと同一サーバ上に Kaspersky Anti-Virus をインストールして使用する場合は、対応しているオペレーティングシステム(Linux、FreeBSD、OpenBSD)とメールシステム(Sendmail、Qmail、Postfix、Exim)がインストールされている必要があります。

平均的な負荷で運用されるメールサーバの場合に、この設定方法をお奨めします。

上記のいずれかのメールシステムと同一のサーバ上で Kaspersky Anti-Virus を使用する場合について、詳しく説明します(**図 2** を参照)。受信メールと送信メールの処理手順は同じであり、以下のように行われます。

1. 他のサーバ(または LAN)から SMTP プロトコル経由でメールメッセージのストリームが送信されてきます。
2. メールシステムがメールトラフィックを受信し、それをスキャンするために Kaspersky Anti-Virus に渡します。
3. アプリケーションが設定に従ってメールトラフィックを処理し、追加の通知と共にそのメールトラフィックをメールシステムに返します。
4. メールシステムが、外部サーバまたは LAN 内のメールボックスにメールトラフィックをルーティングします。

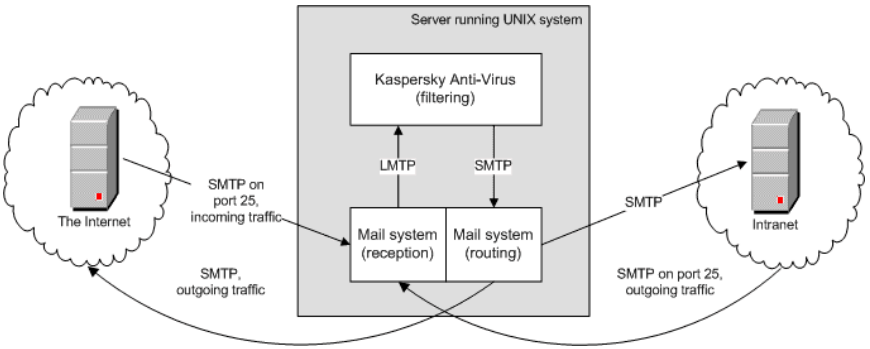

図 2. メールシステムと同一サーバ上で Kaspersky Anti-Virus を使用する場合のダイアグラム

上の図に基づいて、Kaspersky Anti-Virus のインストール中またはインストール後の設定時に、以下の設定を調整する必要があります。

- Kaspersky Anti-Virus が使用するメールサーバポートの設定
- Kaspersky Anti-Virus によるフィルタリング後にメールシステムがメールを受信するためのメールシステムポートの設定

2.3. 2 次フィルタとしての運用

Kaspersky Anti-Virus は、1 次フィルタとしても 2 次フィルタとしても使用できます。使用しているメールサーバにメールトラフィックフィルタが装備されている場合は、Kaspersky Anti-Virus をインストールする際に、どちらのメールフィルタ(Kaspersky Anti-Virus または既存のもの)を 1 次フィルタまたは 2 次フィルタに設定するかを決定する必要があります。これは、2 つのフィルタのフィルタリング方法に基づいて決定します。

1 次フィルタ(MX1 と呼ぶ)は、送信者の IP アドレスに基づいてメールトラフィックをフィルタリングします。このフィルタは、サーバのポート 25 に最初のフィルタとしてインストールされます。1 次フィルタは、入ってくるメールを受信してフィルタリングしてから、2 次フィルタの処理に渡します。*2 次フィルタ*(MX2 と呼ぶ)は、1 次フィルタと同じホストにインストールされますが、別の IP アドレスとポートが割り当てられます。

送信者の IP アドレスに基づくフィルタがサーバにインストールされていない場合は、Kaspersky Anti-Virus を 1 次フィルタとしてインストールできます。IP ベースのフィルタがインストールされている場合は、Kaspersky Anti-Virus を 2 次フィルタとしてインストールします。これは、Kaspersky Anti-Virus によってスキャンされたすべてのメールトラフィックが同一の IP アドレスになるためです。そのため、アンチウイルス処理後に IP に基づいてメールをフィルタリングしても意味がありません。

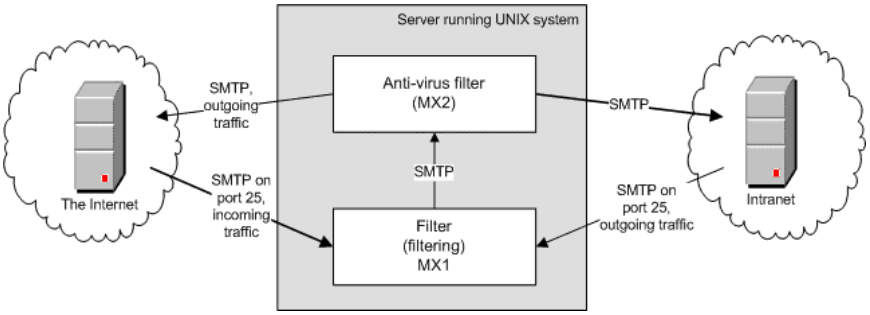

図 3 メールシステムと同一のサーバ上で 2 次フィルタとして Kaspersky Anti-Virus を使用する場合のダイアグラム

1 次フィルタおよび 2 次フィルタについて、以下の設定を行います。

- 1 次フィルタ(MX1)の設定：

  フィルタをインストールするホストの名前：mx1.yourhost.domain

  フィルタの IP アドレス：利用可能なすべてのアドレス

  フィルタが機能するポートの番号：25

  メール送信用のホスト名：mx2.yourhost.domain: 10026

- 2 次フィルタ(MX2)の設定：

  フィルタをインストールするホストの名前：mx2.yourhost.domain

  フィルタの IP アドレス：127.0.0.1

  フィルタが機能するポートの番号：10026

  メールの送信元のホスト名：mx1.yourhost.domain

[helo/ehlo]ダイアログのホスト名が同じだと、サーバがメッセージを受け付けないため、MX1 および MX2 には異なるホスト名を指定する必要があります。MX1 における MX2 のステータスは信頼されている必要があります。その反対も同様です。そうでない場合、配信が失敗します。

2.4. 専用サーバでの運用

使用しているメールサーバで対応していないオペレーティングシステム(Windows など)が稼働している場合でも、Kaspersky Anti-Virus は、フィルタリングおよびアンチウイルス処理を提供できます。
このような場合、Kaspersky Anti-Virus を Linux、FreeBSD、OpenBSD が稼働している専用サーバにインストールしている必要があります。
受信したメールトラフィックを Windows メールサーバに転送するために、この専用サーバにメールシステム(Sendmail、Qmail、Postfix、Exim)をインストールして Kaspersky Anti-Virus と統合する必要があります(28 ページのセクション **4.4** を参照)。
このようにインストールすることにより、以下のように処理が行われます(**図 4** を参照)。

1. Unix ファミリーに属するオペレーティングシステムを稼働しているサーバが、メールトラフィックを受信します。
2. メールシステム(Postfix など)が、スキャン処理のためにそのメールトラ

フィックを LMTP プロトコル経由で Kaspersky Anti-Virus に転送します。

3. スキャンされたメールとアンチウイルスによって作成された通知が、メールシステムに戻され、それらがメインメールサーバに転送されます。その後、送信またはルーティングされます。

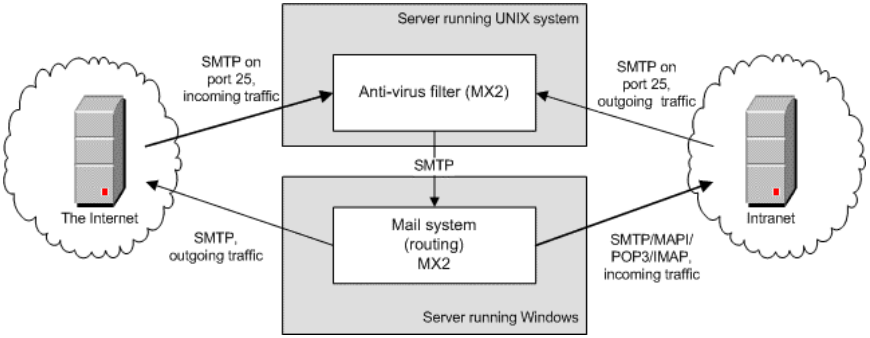

図 4. 専用サーバ上で Kaspersky Anti-Virus を使用する場合のダイアグラム

上の図では、Kaspersky Anti-Virus がインストールされているサーバが、メールトラフィックを受信して再送信しているため、1 次サーバです。一方、Microsoft Exchange がインストールされているサーバは、メール配信のみ行う 2 次サーバです。

ただし、Kaspersky Anti-Virus をインストールする以前に、メールサーバが送信者の IP アドレスに基づいてフィルタリングを行っていた場合は、Kaspersky Anti-Virus をインストールするサーバを 2 次サーバとして定義する必要があります。これは、Kaspersky Anti-Virus をインストールするサーバを 1 次サーバとして定義すると、2 次サーバ(IP ベースのフィルタリングを行う)が受信するメールメッセージの IP アドレスがすべて同じになり、フィルタリングできなくなるためです。

LAN 内に複数のメールサーバがある場合は、MX レコードまたは転送パラメータが 2 次サーバではなく 1 次サーバを指すようにする必要があります。

- 1 次フィルタ(MX1)の設定：

  フィルタをインストールするホストの名前：mx1.yourhost.domain

  メール転送用のホスト名：mx2.yourhost.domain: 25

- 2 次フィルタ(MX2)の設定：

フィルタをインストールするホストの名前：mx2.yourhost.domain
メールの送信元のホスト名：mx1.yourhost.domain

2.5. 外部メールボックスから受信したメールのフィルタリング

最近は、*www.mail.ru*、*www.aport.ru*、*www.hotmail.com* などのウェブメールサーバ上の外部メールボックスがよく使われています。
しかし、そのようなメールボックスから感染メッセージをダウンロードした場合、感染をどのように防いだらよいでしょうか。実際には、このようなメールは POP3 プロトコルを使用して配信されますが、Kaspersky Anti-Virus がスキャンするのは SMTP プロトコルを使用するメールトラフィックのみです。
外部メールのウイルス保護を確実にするためには、以下の設定が必要です。

1. デフォルトの POP3 ポート(110 番)を遮断します。ユーザが外部メールにアクセスできるようにします。そこで、**fetchmail** を使用して、POP3 用のプロキシサーバとしてゲートウェイが動作するようにします。**fetchmail** は、外部サーバからメールメッセージをダウンロードし、それらをローカルの SMTP ポートに送信します。**fetchmail** を使用することにより、SMTP ポートから入ってきたメールメッセージを Kaspersky Anti-Virus がスキャンできるようになります。

   外部メールボックスのメールをフィルタリングするには、fetchmail パッケージがインストールされているコンピュータ上に、ローカル SMTP サーバおよびローカルユーザアカウントが必要です。

   fetchmail は、非常に簡単に設定できます。各ユーザの$HOME ディレクトリに、以下の内容が含まれた*.fetcmailrc* ファイルを作成するだけです。

```
set postmaster "user"
set bouncemail
set no spambounce
set properties ""
poll mail.that.is.free.ru with proto POP3
      user 'remote_user' there with password 'pass12345' is 'user' here
poll mail2.that.is.free.ru with proto POP3
      user 'remote_user2' there with password 'pass123452' is 'user' here
```

各コマンドおよびパラメータの意味は以下の通りです。

user は、ローカルネットワーク上でのユーザの名前です。

mail.that.is.free.ru および *mail2.that.is.free.ru* は、メールを収集する必要があるホストの名前です。

remote_user および *remote_user2* は、それぞれ *mail.that.is.free.ru* および *mail2.that.is.free.ru* のサーバ用のログインです。

pass12345 および *pass123452* は、*remote_user* および *remote_user2* のメールアカウント用のパスワードです。

これらの設定を行うことにより、fetchmail プログラムが *mail.that.is.free.ru* および *mail2.that.is.free.ru* の各ホストからメールメッセージを収集し、それらを *user* のローカル SMTP に送信するようになります。fetchmail は、メッセージのフィールド(*from*、*to*、その他)を一切変えることなく、*received* というヘッダのみ追加します。ユーザには、これらのメールメッセージが通常の方法で受信されたように見えます。

2. crontab を使用して、ユーザの cron ユーティリティが、たとえば 10〜15 分ごとに fetchmail を起動するよう設定します。

外部メールボックスを使用する他のユーザのために、fetchmail プログラムの設定を自動で行うようにするには、以下のデータが必要になります。

- fetchmail によるメールメッセージの収集の対象となる外部ホストの名前
- 外部ホストのログインアカウント
- アカウントのパスワード

さらに、各ユーザのホームディレクトリに、以下の内容が含まれた*.fetchmailrc* ファイルを作成する必要があります。

```
set postmaster "user"
set bouncemail
set no spambounce
set properties ""
```

以下のスクリプトファイルを使用して、メールボックスレコードを追加できます。

```
#!/bin/bash
echo "poll $1 with proto POP3 " >>$HOME/.fetchmailrc
echo "user '$2' with password '$3' is '$4' here">>$HOME/.fetchmailrc
```

pop.mail.ru、*dan*、*secret*、*admin* の各パラメータを指定してこのスクリプトフ

ファイルを実行すると、*dan@mail.ru* というユーザのメッセージが、*admin@your_host.your_domain* というアドレスに転送されます。

第3章 KASPERSKY ANTI-VIRUS のインストール

Kaspersky Anti-Virus をインストールする前に、システムで以下の準備を行ってください。

- 使用しているシステムがハードウェアおよびソフトウェアの要件を満たしていることを確認してください。推奨アプリケーションがインストールされていない場合は、それらをインストールすることをお奨めします。インストールされていないと、アプリケーションの一部の機能が使用できなくなります。
- サーバにインストールされているメールシステムの設定ファイルのバックアップを作成します。
- インターネット接続を設定します。
- Kaspersky Anti-Virus を統合する**メールサーバを停止します。**
- **root** としてシステムにログインします。

アプリケーションのインストール作業は、営業外時間またはメールトラフィックが最も少ない時間帯に行うことをお奨めします。

3.1. Linux が稼働しているサーバへのインストール

Linux システム用の Kaspersky Antivirus には、使用しているオペレーティングシステムの配布方法に応じた 3 種類のインストールパッケージ(rpm、deb、tar.gz)があります。

.rpm パッケージから Kaspersky Anti-Virus のインストールを開始するには、コマンドラインで以下のコマンドを入力します。

rpm –i <distribution_package_filename>

.deb パッケージから Kaspersky Anti-Virus のインストールを開始するには、コマンドラインで以下のコマンドを入力します。

dpkg –i <distribution_package_filename>

また、すべての Linux オペレーティングシステムを対象とした共通の配布ファイルを使用することもできます。使用している Linux のバージョンが RPM または DEB 形式をサポートしていない場合や、ネットワーク管理者が組み込み型パッケージマネージャを使用していない場合に、このファイルを使用します。

Kaspersky Anti-Virus の共通インストールパッケージは、アーカイブ形式で提供されます。このアーカイブのディレクトリツリーには、配布パッケージファイルと、インストールを実行する *install.sh* インストールスクリプトが含まれています。

共通インストールパッケージから Kaspersky Anti-Virus をインストールするには、以下の手順を実行します。

1. アーカイブ形式のインストールパッケージをサーバファイルシステムのディレクトリにコピーして解凍します。
2. インストールスクリプトの *./install.sh* を実行します。

3.2. FreeBSD または OpenBSD が稼働しているサーバへのインストール

FreeBSD または OpenBSD オペレーティングシステムが稼働しているサーバ用の Kaspersky Anti-Virus インストールパッケージは、.pkg パッケージとして提供されます。

.pkg パッケージから Kaspersky Anti-Virus のインストールを開始するには、コマンドラインで以下のコマンドを入力します。

pkg_add <package_name>

3.3. インストール手順

エラーコードが表示されてインストール処理が終了した場合は、使用しているコンピュータがハードウェアおよびソフトウェアの要件を満たしているかどうかと、root としてシステムにログインしているかどうかを確認してください。

サーバ上でアプリケーションをインストールするには、以下の手順を実行しま

す。

1. アプリケーションファイルをサーバにコピーします。
2. ライセンスキーをインストールします。

ライセンスキーがインストールされていないと、設定処理が開始されず、アプリケーションを使用できません。インストール時点でライセンスキーが手元にない場合(たとえば、インターネット経由でアプリケーションを購入したため、電子メールで受け取るライセンスキーがまだ到着していない場合など)、セットアップの完了後、実際にアプリケーションの使用を開始する前に、キーをインストールすることができます。

3. *keepup2date* コンポーネントを設定します。
4. ウイルス定義データベースをインストールして更新します。

アプリケーションの使用を開始する前に、ウイルス定義データベースをインストールしてください。ウイルスのスキャンおよび駆除処理は、ウイルス定義データベースに基づいて行われます。ウイルス定義データベースには、現時点で認識されているすべてのウイルスの説明と、感染オブジェクトの駆除方法が格納されています。ウイルス定義データベースを使用せずにスキャンやファイル処理を実行することはできません。

ウイルス定義データベースがインストールされていないと、アプリケーションの自動設定が実行されないことに注意してください。

5. Webmin モジュールをインストールします。

リモートからソフトウェアを管理するための Webmin モジュールを正しくインストールするには、Webmin アプリケーションをデフォルトのディレクトリに作成する必要があります。Webmin のインストール後に、アプリケーションと連動させるための詳しいモジュールの設定方法を受信できます。

以下のセクションでは、上記の手順について詳しく説明します。

3.4. アプリケーションの設定

サーバにアプリケーションファイルをコピーすると、すぐにインストーラがシステム設定を開始します。パッケージマネージャで対話型スクリプトが許可されている場合は、インストールは自動的に開始されます。許可されていない場合は、手動で開始するようメッセージが表示されます。
インストールでは、以下の処理が行われます。

- インストールされているメールサーバを検索し、そのバージョンをソフトウェア要件と照らし合わせます。
- メールサーバの設定ファイルを検索して変更します。

設定中に追加情報(メールサーバの設定ファイルへのパスなど)が必要になると、サーバのコンソールに情報の要求が発行されます。入力した回答が無効だと、処理が中止されます。
設定処理が正常に終了したら、アプリケーションを使用できます。その場合、インストーラはそれ以上メッセージを表示しません。インストールパッケージに含まれている設定ファイルには、運用を開始するために必要なすべてのパラメータが含まれています。

アプリケーションの使用を開始する前に、メールサーバを再起動してください。

第4章　インストール後の設定

Kaspersky Anti-Virus のインストール中に、インストール先のシステムが解析され、一部のアプリケーションの設定パラメータにはシステムに応じた最適値が自動的に設定されます(25 ページのセクション **4.1** を参照)。

アプリケーションの使用を開始する前に、インストール中にウイルス定義データベースのインストールまたは更新が実行されなかった場合は実行し、サーバファイルシステムのウイルススキャンを行うことをお奨めします。

しかし、それだけではプログラムの使用を開始できません。以下の手順を実行する必要があります。

- Kaspersky Anti-Virus をサーバにインストールされているメールシステムと統合します。
- 送受信メールのウイルススキャンおよび駆除を行うライセンスユーザのリストを作成します。

さらに、Kaspersky Anti-Virus と Webmin パッケージが連動するよう設定することをお奨めします。

この章では、Kaspersky Anti-Virus のデフォルト設定について説明してから、アプリケーションの使用に必要な設定について詳しく説明します。

以降の例では、Linux ディストリビューションの一般的なパスが示されています。

4.1. アプリケーションのデフォルト設定

Kaspersky Anti-Virus のすべてのパラメータは、*/etc/kav/5.5kav4mailservers.conf* というデフォルト設定ファイルに格納されます。

独自の設定ファイルを作成し、それを使用して現在のタスクを実行したり、デフォルト設定ファイルとして使用したりすることもできます。

このセクションでは、このファイルに設定されているデフォルトのパラメータ値について詳しく説明します。この章を読めば、各企業の環境条件において Kaspersky Anti-Virus の追加設定(58 ページの**第 6 章**を参照)が必要かどうかを判断できます。

サーバファイルシステムのウイルス保護

Kaspersky Anti-Virus のデフォルト設定では、コマンドラインスイッチを使用せずに *kavscanner* コンポーネントを起動すると、現在の場所から再帰的にサーバディレクトリおよびファイルシステムのウイルススキャンが実行されます。

感染ファイル、感染の疑いがあるファイル、または破損ファイルが検出されると、対応するメッセージがコンソールおよびレポートファイルに送信されます。

デフォルトでは、Kaspersky Anti-Virus によって検出された感染ファイルは駆除されないことに注意してください。

サーバのメールトラフィックのウイルス保護

Kaspersky Anti-Virus とメールシステムとウイルス保護を統合しない限り、メールトラフィックのウイルス保護を行うことはできません。以下では、アプリケーションがメールシステムと統合されている場合の、アプリケーションのデフォルト処理を指定する設定について説明します。

kav4mailservers.conf 設定ファイルの**[smtpscan.group:default]**セクションは、**default** グループを定義します。このグループには、保護対象のすべてのメールサーバユーザが含まれます。このグループは、ウイルススキャンおよびメールトラフィックの処理について以下のルールを設定します。

- 受信メールおよび送信メールのメッセージがスキャンされます。
- 感染メールメッセージが検出された場合、アプリケーションによりそれらが駆除されます。

  駆除後のメールメッセージは、ウイルスが含まれていたことと、その駆除に成功したことを知らせる通知と共に、受信者およびグループ管理者(*postmaster@localhost*)に配信されます。また、同様のメッセージがメッセージ作成者にも送信されます。

  メッセージのウイルスを駆除できなかった場合、メッセージが削除され、それに関する通知が受信者、送信者、およびグループ管理者に送信されます。

メールメッセージのスキャン、駆除、削除、および隔離などに関する通知は、デフォルトではすべて *MAILER-DAEMON@localhost* というアドレスから送信されます。

- メールトラフィックのウイルススキャンでは、感染の疑いがあるファイル、破損ファイル、パスワードで保護されたファイル、およびスキャンできないメールメッセージは、削除されます。そのことを知らせる通知が、受信者、送信者、およびグループ管理者に送信されます。
- アプリケーションによって行われた処置は、レポートファイルにすべて記録されます。

メールトラフィックのウイルススキャンを行うには、*aveserver* 処理が実行されていなければなりません。この処理が無効になっている場合、すべての受信メールトラフィックが、スキャンおよび処理のために自動的にキューに作成されます。これに関する情報が、アプリケーションのログファイルに保存されます。73 ページのセクション **6.5** を参照してください。

4.2. ウイルス定義データベースのインストール/更新

アプリケーションをインストールしたら、すぐにウイルス定義データベースのインストールおよび更新を行うことをお奨めします。
インストール/更新を行うには、*keepup2date* コンポーネントを実行します。コマンドラインで、以下のコマンドを入力します。

/opt/kav/5.5./kav4mailservers/bin

カスペルスキーラブスの更新サーバからウイルス定義データベースがダウンロードされて、設定ファイルで指定されているディレクトリに保存されます。

ウイルス定義データベースを 1 時間おきに更新することをお奨めします。日々新種のウイルスが出現するため、アプリケーションを最新の状態にしておく必要があります。データベース更新の詳細については、37 ～ 38 ページのセクション **5.1.3** ～ **5.1.4** を参照してください。

4.3. Webmin との連動設定

Kaspersky Anti-Virus をリモートで制御する場合は、アプリケーションが

Webmin パッケージと連動するよう設定することをお奨めします。
たとえば、Webmin を使用してユーザパスワードを設定することにより、プログラムへのアクセスを制限することができます。Webmin の設定方法の詳細については、Webmin に付属のマニュアルを参照してください。
Webmin からリモートで変更されたアプリケーション設定は、すべてアプリケーションのデフォルト設定ファイルに保存されます。

Webmin を使用してデフォルト以外の設定ファイルを作成したい場合は、以下の手順を実行する必要があります。

- 既存の設定ファイルのデータをコピーして新しい設定ファイルを作成し、違う名前を付けて保存します。その後で、必要に応じて新しい(代替) 設定ファイルを変更します。
- **[Config edit]**タブの**[Full path to KAV config]**パラメータの入力フィールドで、代替設定ファイルの名前を指定します。

4.4. 手動でメールシステムと統合する

アプリケーションのインストール中に setup.sh スクリプトが使用されなかった場合、つまりアプリケーションが自動で設定されなかった場合のみ、以下の手順を行ってください。

手動で統合する場合、以下の手順を実行します。

1. Kaspersky Anti-Virus と連動するように、メールシステムの設定を調整します。
2. メールシステムと確実に連動するように、アプリケーションの設定を調整します。
3. 新しい設定を使用してメールシステムを起動します。

メールシステムの起動および操作に使用されるアカウントを持つユーザは、各メールシステムの設定ファイルの読み取り権限を持っている必要があります。

以下のサブセクションでは、Kaspersky Anti-Virus をサポート対象メールシステムと手動で統合する場合について説明します。

4.4.1. Sendmail との統合

Kaspersky Anti-Virus を Sendmail に統合するには、以下の手順を実行します。

1. *sendmail.cf.listen* を *sendmail.cf.*ファイルにコピーします。
2. 新しい *sendmail.cf.listen* ファイル内に、以下のような 98 番目のル

ールを作成します。

SParseLocal=98

R$*[tab_character]$#smtpscanner $@$1 $:$1

3. さらにこのファイル内に、*smtpscanner* の記述を入力します。

Msmtpscanner,
P= /opt/kav/5.5./kav4mailservers/bin/smtpscanner,
F=PCXmnz9, S=EnvFromSMTP, R=EnvToSMTP,
E=\r\n, L=2040,
T=SMTP,
A=smtpscanner

4. 必要に応じて Kaspersky Anti-Virus を設定します(32 ページのセクション **4.4.5** を参照)。
5. 起動スクリプトに以下の 2 つの処理を追加します。

/usr/sbin/sendmail –bd –q10m –C /etc/mail/sendmail.cf.listen
/usr/sbin/sendmail –C /etc/mail/sendmail.cf

submit.cf を編集して Sendmail バージョン 8.12 を使用する場合は、以下の 3 つの処理を起動スクリプトに追加します。

/usr/sbin/sendmail –bd –q10m –C /etc/mail/sendmail.cf.listen
/usr/sbin/sendmail –C /etc/mail/sendmail.cf
/usr/sbin/sendmail –C /etc/mail/submit.cf

4.4.2. Qmail との統合

Kaspersky Anti-Virus を Qmail メールシステムに統合する場合、*smtpscanner* コンポーネントにより *qmail-queue* プログラムが置き換えられます。メッセージを送信したりキューに配置したりする場合は、*smtpscanner* が元の *qmail-queue* プログラムを呼び出します。

Kaspersky Anti-Virus を Qmail に統合するには、以下の手順を実行します。

1. **/var/qmail/bin/**ディレクトリ内の *qmail-queue* ファイルの名前を *queue.kav55* に変更します。
2. **/opt/kav/5.5/kav4mailservers/bin/**ディレクトリ内の *qmail-queue* ファイルを**/var/qmail/bin** ディレクトリにコピーするか、またはこのファイルへのシンボリックリンクを作成します。
3. *qmail-queue* および *qmail kav55* ファイルにアクセスするための権限を以下のように設定します。

16 -rws—x—x 1 qmailq qmail 12688 Mar 24 13:56 qmail-que
316 –rwx—x—x 1 qmailq qmail 315612 Apr 14 11:29 qmail-queue

4. 必要に応じて Kaspersky Anti-Virus を設定します(32 ページのセクション **4.4.5** を参照)。
5. メールシステムを再起動します。

Qmail システムで *softlimit* ユーティリティが使用される場合、使用可能なメモリ容量を増加するか、またはメモリ制限を無効にする必要があります。そうしないと、大きな電子メールメッセージをスキャンする際に、問題が発生する可能性があります。

4.4.3. Postfix との統合

Kaspersky Anti-Virus を Postfix に統合するには、以下の手順を実行します。

1. 使用している Postfix メールシステムのバージョン番号を確認します。**snapshot_20000529** よりも新しいバージョンである必要があります。Postfix の Web サイト(www.postfix.org)から最新版をダウンロードしてください。
2. Postfix メールシステムの設定ファイル *main.cf* に、以下の内容を追加します。

   content_filter = lmtp:localhost:10025
3. Postfix メールシステムの設定ファイルである *master.cf* に、以下の内容を追加します。

   localhost:10025 inet n n n - 10 spawn user=filter argv=/opt/kav/bin/smtpscanner

   localhost:10026 inet n - n - 10 smtpd -o content_filter= -o myhostname=localhost
4. **/var/spool/filter** ディレクトリを作成します。**filter** というユーザを作成し、**/var/spool/filter** をホームディレクトリとして指定して、**filter** グループにこのアカウントを追加します。それに応じて、このディレクトリへのアクセス権限を変更します。*smtpscanner* は、**filter** ユーザアカウントに割り当てられている権限を使用して動作することに注意してください。

   mkdir /var/spool/filter

   groupadd filter

   useradd filter –s /bin/false –d /var/spool/filter –g filter

   chown filter.filter /var/spool/filter
5. 必要に応じて Kaspersky Anti-Virus を設定します(32 ページのセク

ション **4.4.5** を参照)。

6. メールシステムを再起動します。

4.4.4. Exim との統合

Kaspersky Anti-Virus を Exim に統合するには、以下の手順を実行します。

1. 設定ファイル(*exim.conf* など)を *exim.conf.listen* にコピーします。
2. *exim.conf:listen* ファイルに以下の修正を加えます。
   - TRANSPORT CONFIGURATION セクションに以下の内容を追加します。

     ```
     kav_lmtp_transport:
        driver = lmtp
        command = /opt/kav/bin/smtpscanner
     ```

   - ROUTERS CONFIGURATION セクションで、以下のローカルメール配信パラメータを定義します。

     ```
     localuser:
          driver=accept
          transport=kav_lmtp_transport
     ```

     リモートメール配信用のパラメータを設定します。

     ```
     lookuphost:
          driver=dnslookup
          transport=kav_lmtp_transport
     ```

3. 必要に応じて Kaspersky Anti-Virus を設定します(32 ページのセクション **4.4.5** を参照)。
4. 起動スクリプトに以下の 2 つの処理を追加します。

   ```
   exim -q10m -bd –C /etc/exim/exim.conf.listen
   exim -C /etc/exim/exim.conf
   ```

smtpscanner コンポーネントを別のユーザアカウントから起動できるようにしたい場合は、EXIM_GID および EXIM_UID パラメータに別の値を指定して Exim メールシステムをコンパイルしてください。詳細については、Exim メールシステムのマニュアルを参照してください。

4.4.5. メールシステムと統合するための Kaspersky Anti-Virus の設定

Kaspersky Anti-Virus をメールシステムと統合するために行う必要があるもう 1 つの作業は、アンチウイルスプログラム自体の設定ファイルを編集する作業です。

メールシステムと連動するよう Kaspersky Anti-Virus を設定するには、以下の手順を実行します。

Kaspersky Anti-Virus の設定ファイルで以下の設定を行います。

- 通知の送信元アドレスを指定します。

  NotifyFromAddress=admin@yourhostname.ru

- **[smtpscan.general]**セクションで、メールシステムの ID を設定します。メールシステムの ID は、**protocol:host:port** という構造で設定します。各部の意味は以下の通りです。

  protocol は、メールの送信に使用されるプロトコルです(**smtp** または **lmtp**)。

  host は、メールの送信元になるホストの名前または IP アドレス、もしくはメールプログラムの名前です。

- 使用するプロトコル(LMTP または SMTP)を選択します。

  メールプログラムへの完全パスを丸カッコで囲んで指定します。任意のコマンドラインオプションを含めることもできます。

  port – ポート番号です(デフォルトではポート 25)。

  たとえば、以下のようになります。

  smtp:localhost.tu:1100 または **lmtp:(local.mail –l)**

  - Sendmail の場合：

    ForwardMailer=smtp:(/usr/sbin/sendmail –bs –C /etc/mail/sendmail.cf)

  - Qmail の場合：

    ForwardMailer=qmail:(/var/qmail/bin/qmail-que)

  - Postfix の場合：

    ForwardMailer=smtp:localhost:10026

- Exim の場合：

  ForwardMailer=smtp:(exim –bs
  -C/etc/exim/exim.conf)

- ユーザのグループについて、設定ファイルの**[smtpscan.group:default]**セクションで以下のように指定します。

  AdminAddress=admin@yourhostname.ru
  AdminNotify=yes

- **[smtpscan.limits]**セクションで、aveserver 処理のタイムアウト時間(秒単位)をたとえば以下のように設定します。

  MaxCheckTime=60

第5章 KASPERSKY ANTI-VIRUS の使用

Kaspersky Anti-Virus を使用すると、サーバに保存されているファイルから、外部メールボックスから収集されるメールを含む送受信メールトラフィックまで、サーバをウイルスから完全に保護することができます。
アプリケーションのユーティリティが各タスクに用意されており、管理者はそれを使用して作業できます。Kaspersky Anti-Virus によって実行されるタスクは、以下の 3 種類に分けられます。

1. ウイルスのスキャンおよび感染オブジェクトの駆除に使用されるウイルス定義データベースの更新
2. サーバのメールトラフィックについてのウイルス保護
3. サーバのファイルシステムについてのウイルス保護

上記の各グループは、アプリケーションの特定機能を使用する具体的なタスクによって設定されます。この章では、最も一般的なタスクを想定して解説を行います。管理者は、それぞれの業務要件に合わせてこれらのタスクを組み合わせたり複雑にしたりできます。
ここでは、コマンドラインを使用してローカルでタスクを設定および実行する方法について説明します。

以下で説明されているすべてのタスクは、管理者がインストール後の設定を完了していることを前提としています(25 ページの**第 4 章**を参照)。

メールのウイルススキャンに関するタスクを実行する前に、オペレーティングシステムの起動時に *aveserver* 処理がロードされていない場合は、この処理を起動する必要があります。

5.1. ウイルス定義データベースの更新

アプリケーションの *keepup2date* コンポーネントは、ウイルス定義データベースを最新の状態にしておくために欠かせない機能を実行します。Kaspersky Anti-Virus は、このウイルス定義データベースを使用してスキャンおよび感染オブジェクトの駆除を行います。ウイルス定義データベースは、以下のアドレスにあるカスペルスキーラブスの更新サーバからダウンロードできます。

http://downloads1.kaspersky-labs.com/updates/

http://downloads2.kaspersky-labs.com/updates/

ftp://downloads1.kaspersky-labs.com/updates/、およびその他のサーバ

更新をダウンロードできるすべてのアドレスが掲載されたリストは、アプリケーションパッケージに含まれている *updcfg.xml* ファイル内にあります。このリストは、定期的に自動更新されます。

updcfg.xml ファイルを手動で編集することはできません。

更新処理中に、*keepup2date* コンポーネントがこのファイル内のサーバリストからアドレスを 1 つ選び、対応するサーバからウイルス定義データベースをダウンロードしようとします。そのアドレスからのダウンロードに失敗した場合、*keepup2date* はリスト内の次のアドレスを使用して処理を繰り返します。更新が成功すると、デフォルトではアプリケーションが自動的に再起動されます(**[updater.options]**セクションの **PostUpdateCmd** パラメータ)。

keepup2date コンポーネントの設定は、すべて設定ファイルの **[updater.*]**オプションに格納されています。

複雑な LAN 構造を使用している場合は、ウイルス定義データベースの更新をネットワークディレクトリにいったんダウンロードしてから、他のネットワークコンピュータがそのディレクトリから更新をコピーするよう設定することをお奨めします。

ウイルス定義データベースを 1 時間おきに更新することを強くお奨めします。

cron ユーティリティを使用すると、更新処理を自動で行うことができます(37 ページのセクション **5.1.3** を参照)。管理者がコマンドラインから手動で実行することもできます(38 ページのセクション **5.1.4** を参照)。

5.1.1. *keepup2date* アプリケーションコンポーネント

ウイルス定義データベースを更新する *keepup2date* コンポーネントは、旧バージョンで使用されていた *kavupdater* コンポーネントに代わるものです。

Kaspersky Anti-Virus バージョン *5.5* では、ウイルス定義データベースの更新を行うコンポーネントが差し替えられました。新しいコンポーネントは、以下のように既存の機能が改良され、新しい機能も追加されました。

- 設定ファイルで指定されている地域に基づいて、地理的に最も近くにある更新サーバを自動的に選択するオプション。

- 累積更新がある場合に、増分更新をダウンロードしてインストールするオプション。このオプションは、トラフィックを節約できるため便利です。
- ウイルス定義データベースのダウンロード中に接続が切れた場合や更新サーバが変更された場合の復旧機能。ダウンロード再開後、ウイルス定義データベースを最初からではなく残りの部分のみダウンロードできます。
- ウイルス定義データベースの更新成功後の自動適用。
- 前回のバージョンのウイルス定義データベースに戻すロールバック機能。
- 新しいコンポーネントの操作では、wget プログラムは必要ありません。
- Samba サーバ、Microsoft Windows が稼働しているコンピュータ上の共有ディレクトリから LAN 内コンピュータのウイルス定義データベースを更新できます。

5.1.2. keepup2date コンポーネントの推奨設定

kavupdater コンポーネントには、不要になるパラメータがあります。設定ファイルから手動で削除することをお奨めします。ただし、プロキシアドレスなどの一部のオプションが *keepup2date* でも重要なオプションである場合は、コンポーネントの新しいセクションにコピーする必要があります。

*不要になったため設定ファイルから削除する必要があるパラメータは、**[updater.options]** セクションにあります。*

- **RandomServerOrder** – サーバの選択方法が変わったため、このオプションは使用できません。
- **ReloadApplication** – このオプションの代わりに、**PostUpdateCmd** スクリプトの実行が可能な、より全般的なオプションが追加されました。
- **ExtraWgetOptions** – コンポーネントが外部プログラムとして *wget* を使用しなくなりました。
- **ShowExternalCmdOutput** – 新しいコンポーネントは、外部コマンドを実行しません。

また、サーバのリストが動的に更新されるようになったため、新しいコンポーネントは、**[path]**セクションの **UpdateServersFile** オプションを使用しません。

ウイルス定義データベースは、さまざまな方法で更新できます。ここでは、その更新方法について詳しく説明します。

keepup2date コンポーネント内にリストされているカスペルスキーラブスのサーバの内、いずれか 1 つから更新をダウンロードするようプログラムを設定するには、以下の操作を行います。

[updater.options]セクションの **UseUpdateServerUrl** パラメータに **No** を割り当てます。

ユーザが定義したサーバから更新をダウンロードし、もしもそのサーバにアクセスできない場合は更新を中止するようプログラムを設定するには、以下の操作を行います。

[updater.options] セクションの **UseUpdateServerUrl** および **UseUpdateServerUrlOnly** パラメータに **Yes** を割り当てます。さらに、**UpdateServerUrl** パラメータに、更新をダウンロードするサーバのアドレスを指定する必要があります。

ユーザが定義したサーバから更新をダウンロードし、もしもそのサーバにアクセスできない場合は keepup2date コンポーネント内にリストされているサーバから更新をダウンロードするようプログラムを設定できます。そうするには、以下の操作を行います。

[updater.options]セクションの **UseUpdateServerUrl** パラメータに **Yes** を割り当て、**UseUpdateServerUrlOnly** パラメータには **No** を割り当てます。さらに、**UpdateServerUrl** パラメータに、更新をダウンロードするサーバのアドレスを指定する必要があります。

5.1.3. cron を使用したウイルス定義データベースの自動更新

cron ユーティリティを使用して、ウイルス定義データベースの自動更新を定期的に行うことができます。

行うこと：毎日 3 時間おきにウイルス定義データベースの自動更新が実行されるよう設定。更新サーバは、ランダムに選択されるようにします。*aveserver* 処理は、データベースの更新後に自動的に再起動される必要があります。更新に関するエラーのみシステムログに記録されるようにします。タスクの実行に関する全般的なログを保存します。コンソールには何も出力しないでください。

方法：このタスクを完了するには、以下の手順を実行します。

1. アプリケーション設定ファイルで、以下のように適切な値を定義します。

   [updater.options]
   KeepSilent=yes
   [updater.report]
   Append=yes
   ReportLevel=1

2. cron 処理(**crontab –e**)のルールを定義するファイルに、以下の内容を追加します。

   0 */3 * * * /opt/kav/5.5/kav4mailservers /bin/keepup2date

5.1.4. ウイルス定義データベースの手動更新

ウイルス定義データベースの更新処理は、コマンドラインからいつでも開始できます。

行うこと：ウイルス定義データベースの更新処理を開始し、*/tmp/updatesreport.log* ファイルに結果のレポートを作成。

方法：コマンドラインで、以下のコマンドを入力します。

keepup2date –l /tmp/updatesreport.log

複数のコンピュータ上のウイルス定義データベースを更新する必要がある場合は、各コンピュータがそれぞれにファイルをダウンロードするよりも、1 台のサーバがデータベースをダウンロードしてネットワークディレクトリに保存し、そのディレクトリを使用してすべてのコンピュータを更新する方が便利です。

行うこと：**/home/bases** 共有ネットワークディレクトリ内のファイルを使用してウイルス定義データベースを更新するよう設定。このディレクトリにアクセスできない場合やディレクトリが空の場合は、カスペルスキーラブスの更新サーバを使用して更新処理を行います。作業結果をレポートファイルに出力します。

方法：このタスクを完了するには、以下の手順を実行します。

1. アプリケーション設定ファイルで、以下のように適切な値を設定します。

   [updater.options]
   UpdateServerUrl=/home/bases
   UseUpdateServerUrl=yes

UseUpdateServerUrlOnly=no

(もしくは、–g /home/bases コマンドラインオプションを使用)

2. コマンドラインで、以下のコマンドを入力します。

   keepup2date –l /tmp/report.txt

5.1.5. ウイルス定義データベース用のネットワークディレクトリを作成する

ウイルス定義データベースの更新が、LAN 内の共有ネットワークディレクトリからローカルコンピュータに正しく配布されるようにするために、ネットワークディレクトリ内のファイル構造をカスペルスキーラブスの更新サーバのファイル構造とまったく同じにする必要があります。このセクションでは、ネットワークディレクトリの作成方法について説明します。

行うこと：LAN 内のコンピュータが更新のソースとして使用するネットワークディレクトリを作成します。

方法：このタスクを完了するには、以下の手順を実行します。

1. ローカルディレクトリを作成します。
2. 以下のコマンドを使用して、*keepup2date* コンポーネントを起動します。

   keepup2date –u rdir

   rdir は、作成されたディレクトリへの完全パスです。
3. LAN 上のコンピュータにこのディレクトリへのアクセス権限を付与します。

行うこと：プロキシサーバを使用してウイルス定義データベースを更新するよう設定します。

方法：このタスクを完了するには、以下の手順を実行します。

1. 設定ファイルの**[updater.options]**セクションの **UseProxy** パラメータに **Yes** を割り当てます。
2. 設定ファイルの**[updater.options]**セクションの **ProxyAddress** パラメータに、プロキシサーバのアドレスがあることを確認します。アドレスは、**http://username:password@ip_address:port** の形式に従って指定します。**ip_address** および **port** の値は必須ですが、**username** および **password** の値は、プロキシで認証が必要な場合のみ指定する必要があります。

もしくは、以下の手順を実行します。

1. 設定ファイルの**[updater.options]**セクションの **UseProxy** パラメータに **Yes** を割り当てます。
2. **http://username:password@ip_address:port** の形式に従って **http_proxy** 環境変数を指定します。**[updater.options]**セクションの **UseProxy** パラメータが存在しないかまたは **Yes** が設定されている場合のみ、この変数が使用されます。

5.2. サーバのメールトラフィックについてのウイルス保護

Kaspersky Anti-Virus の最も重要なタスクは、送受信または転送されるメールトラフィックのウイルスをフィルタリングすることです。*smtpscanner* コンポーネントがこのタスクを実行します。
このコンポーネントは、感染メールからユーザを保護し、感染していないメッセージと駆除済みのメッセージをメッセージの検査に関する通知と共にユーザに配信します。
さらに、添付ファイルの形式に応じたフィルタリングオプションを使用することにより、メールトラフィック処理中のサーバの負荷を軽減できます。
Kaspersky Anti-Virus のその他の機能については、以下のメールトラフィックの保護タスクに関するセクションの中で説明します。

smtpscanner コンポーネントの設定は、すべて *kav4mailservers.conf* 設定ファイルの**[smtpscan.*]**オプション内にグループ化されています。

以下の各セクションでは、メールトラフィックのウイルス保護に関する一般的なタスクを説明します。

メールトラフィックのウイルススキャンを行うには、*aveserver* 処理が実行されていなければなりません。

5.2.1. 感染していないメッセージおよび駆除済みメッセージの配信

ユーザを送信者グループや受信者グループに分けない場合に、この設定方法を使用します。たとえば、単純にすべてのサーバアカウントの感染していないメッセージおよび駆除済みメッセージのみを配信する必要がある場合に、この方法が便利です。

行うこと：

- サーバのすべてのメールトラフィックをウイルススキャンし、すべての感染メッセージを駆除します。
- 駆除できない感染メッセージを削除します。
- 駆除済みメッセージを受信者に配信します。
- 駆除が行われたメッセージ、削除されたメッセージ、感染の疑いがあるメッセージ、破損メッセージ、およびチェックできなかったメッセージについて、送信者、受信者、および管理者に通知します。管理者への通知には、感染オブジェクトをそのまま添付します。
- すべての動作を*/tmp/report.log* ファイルに記録します。

方法：このタスクを完了するには、以下の手順を実行します。

1. **[smtpscan.group:default]**グループのパラメータを以下のように設定します。

```
[smtpscan.group:default]
Check=yes
AdminAddress=admin@localhost.ru
AdminNotify=yes
AdminAction=unchanged
SenderNotify=yes
RecipientNotify=yes
RecipientAttachReport=yes
RecipientAction=remove
CuredRecipientNotify=yes
CuredRecipientAttachReport=yes
CuredRecipientAction=cured
```

Sender*、**Recipient***、および **Admin***の各パラメータは、ステータスが **Clear** 以外のすべてのオブジェクト形式を処理するためのルールを定義します。特定のオブジェクト用に設定されたルールは、優先順位が高くなります。したがって、この例では、**駆除済み**オブジェクト(**CuredRecipientAction=cured**)以外のすべてのオブジェクト形式が、受信者のメールから削除されます(**RecipientAction=remove**)。

2. コンポーネントの作業結果が*/tmp/report.log* ファイルに記録されるよう設定します。

   [smtpscan.report]
   ShowOk=yes
   ReportFileName=/tmp/report.log
   ReportFilePermission=0660

5.2.2. 感染メッセージの配信

場合によっては、感染メッセージを含むすべてのメッセージを特定のユーザグループに配信する必要があります。

行うこと：

- すべてのメールトラフィックをウイルススキャンします。
- **urgent** グループ以外のすべてのユーザの感染メッセージを駆除します。
- **urgent** グループ以外の、すべてのユーザの駆除できなかったメールメッセージ、感染の疑いがあるメール、および破損メールを、隔離ディレクトリに移動します。
- ブロックされたメッセージ、駆除が行われたメッセージ、削除されたメッセージ、感染の疑いがあるメッセージ、破損メッセージ、およびチェックできなかったメッセージについて、送信者、受信者、および管理者に通知します。管理者への通知には、感染オブジェクトをそのまま添付します。
- ウイルス感染の可能性があることを知らせる通知を必ず付けて、感染メッセージを含むすべてのメッセージを **urgent** グループの受信者に配信します。

このタスクを完了するには、以下の手順を実行します。

1. **[smtpscan.group:default]**グループの設定設定を以下のように指定します。

   [smtpscan.group:default]

Check=yes
QuarantinePath=/var/db/Quarantine
Quarantine=yes
InfectedQuarantine=yes
SuspiciousQuarantine=yes
CorruptedQuarantine=yes
ErrorQuarantine=yes
ProtectedQuarantine=yes
AdminAddress=admin@localhost.ru
AdminNotify=yes
AdminAction=unchanged
SenderNotify=yes
RecipientNotify=yes
RecipientAttachReport=yes
RecipientAction=remove
CuredRecipientNotify=yes
CuredRecipientAttachReport=yes
CuredRecipientAction=cured

2. **[smtpscan.group:urgent]グループ**の設定を以下のように設定します。

[smtpscan.group:urgent]
Check=yes
Quarantine=no
AdminAddress=admin@localhost.ru
AdminNotify=yes
AdminAction=unchanged
SenderNotify=yes
RecipientNotify=yes
RecipientAttachReport=yes
RecipientAction=unchanged

5.2.3. パスワードで保護されたアーカイブを含むメッセージの配信

電子メールメッセージには、パスワードで保護されたアーカイブファイルが添

付されていることがよくあります。Kaspersky Anti-Virus は、アーカイブに含まれている感染ファイルの駆除は行いません。したがって、デフォルトでは、パスワードで保護されたアーカイブはスキャンされずに配信されます。その場合、アーカイブがスキャンされていないことを知らせるメッセージが生成されます。生成された通知は、メッセージの受信者および管理者に送信されます。

チェックされていないアーカイブの配信を知らせる通知を無効にするには、以下の手順を実行します。

- アプリケーション設定ファイルの**[smtpscan.group:default]**セクションで、**ProtectedRecipientAttachReport** パラメータに **no** を割り当てます。それにより、受信者への通知の配信が無効になります。
- **[smtpscan.group:default]**セクションの **ProtectedAdminNotify** パラメータに **no** を割り当てます。それにより、グループ管理者への通知の配信が無効になります。

5.2.4. 受信者へのメッセージ配信をブロックする

通常、管理者はメッセージ配信をブロックする必要がある場合があります。たとえば、重要なデータが含まれているメールメッセージがウイルスに感染している疑いがある場合などです。駆除処理を行うと、データが失われる可能性があります。そのような場合は、メールメッセージを隔離して、たとえばカスペルスキーラブスに送信して専門家に分析を依頼するなどします。

行うこと：

- サーバのすべてのメールトラフィックについてウイルスをスキャンし、すべての感染メッセージを駆除します。
- 感染メッセージ、感染の疑いがあるメッセージ、破損メッセージ、パスワードで保護されたメッセージ、およびスキャンできないメッセージの配信をブロックします。
- 感染していないメッセージまたは駆除済みメッセージのみ受信者に配信します。
- ブロックされたメッセージ、駆除が行われたメッセージ、削除されたメッセージ、感染の疑いがあるメッセージ、破損メッセージ、およびチェックできなかったメッセージについて、送信者、受信者、および管理者に通知します。管理者への通知には、感染オブジェクトをそのまま添付します。

方法：このタスクを完了するには、以下の手順を実行します。

kav4mailservers.conf 設定ファイルで以下の設定を行います。

```
[smtpscan.group:default]
Check=yes
QuarantinePath=/var/db/Quarantine
Quarantine=yes
InfectedQuarantine=yes
SuspiciousQuarantine=yes
CorruptedQuarantine=yes
ErrorQuarantine=yes
ProtectedQuarantine=yes
AdminAddress=admin@localhost.ru
AdminNotify=yes
AdminAction=unchanged
SenderNotify=yes
RecipientNotify=yes
RecipientAttachReport=yes
```

RecipientAction=remove
CuredRecipientNotify=yes
CuredRecipientAttachReport=yes
CuredRecipientAction=cured

5.2.5. 添付ファイルの種類に基づくメッセージのフィルタリング

ウイルスを含む危険性のあるファイル(.exe ファイルなど)がメールに添付されていることがよくあります。感染を防ぐために、このようなオブジェクトの名前や形式に基づいてメールトラフィックをフィルタリングし、ブロックされた添付ファイルを別のディレクトリに移動して詳しく分析することをお奨めします。
また、中には感染しないオブジェクトもあります。メールメッセージのアンチウイルス処理中のサーバの負荷を軽減するために、これらのファイルを形式や名前に基づいて事前に検出し、メールチェック中はそれらのファイルを別にしておくことをお奨めします。

行うこと：

- **users** グループの場合：
  - グループのメールメッセージのウイルスをスキャンします。
  - メールメッセージに添付されている.exe ファイルをフィルタで検出します。検出されたファイルを特別なディレクトリに隔離します。
  - 感染したメールメッセージがある場合は駆除します。オブジェクトの駆除が失敗した場合は、メッセージからオブジェクトを削除しますが、グループ管理者には削除せずにメッセージをそのまま配信します。
  - グループ管理者および受信者にのみブロックされたオブジェクトについて通知します。
  - 削除メッセージ、感染メッセージ、破損メッセージ、パスワードで保護されたメッセージ、およびスキャンできないメッセージについて、管理者、送信者、および受信者に通知します。

- その他のすべての受信者の場合：
  - すべてのメールトラフィックについてウイルスをスキャンし、すべての感染メッセージを駆除します。
  - 駆除できない感染メッセージ、感染の疑いがあるメッセージ、破損メッセージ/オブジェクト、およびスキャンできないオブジェクトを隔離します。
  - 駆除済みメッセージを受信者に配信します。
  - パスワードで保護されたファイルを、ウイルス感染の可能性についての通知と共に受信者に配信します。
  - 削除メッセージ、感染メッセージ、破損メッセージ、ブロックされたメッセージ、およびスキャンできないメッセージについて、送信者、受信者、および管理者に通知します。管理者への通知には、すべての形式のオブジェクトがそのまま添付されます。

このタスクを完了するには、以下の手順を実行します。

1. **[smtpscan.group:users]**グループの設定を以下のように設定します。

```
[smtpscan.group:users]
Check=yes
QuarantinePath=/var/db/Quarantine
Quarantine=yes
AdminAddress=admin@localhost.ru
AdminNotify=yes
AdminAction=unchanged
SenderNotify=yes
RecipientNotify=yes
RecipientAttachReport=yes
RecipientAction=remove
FilterName=*.exe$
FilteredQuarantine=yes
FilteredRecipientNotify=yes
CuredRecipientNotify=yes
CuredRecipientAttachReport=yes
```

CuredRecipientAction=cured
ProtectedRecipientNotify=yes
ProtectedRecipientAction=unchanged
ProtectedRecipientAttachReport=no
ProtectedSenderNotify=no
ProtectedAdminNotify=no

2. **[smtpscan.group:default]**グループの設定を以下のようにします。

Check=yes
QuarantinePath=/var/db/Quarantine
Quarantine=yes
InfectedQuarantine=yes
SuspiciousQuarantine=yes
CorruptedQuarantine=yes
ErrorQuarantine=yes
AdminAddress=admin2@localhost.ru
AdminNotify=yes
AdminAction=unchanged
SenderNotify=yes
RecipientNotify=yes
RecipientAttachReport=no
RecipientAction=remove
ProtectedRecipientNotify=yes
ProtectedRecipientAttachReport=yes
ProtectedRecipientAction=unchanged
CuredRecipientNotify=yes
CuredRecipientAttachReport=yes
CuredRecipientAction=cured

ユーザグループの作成については、60 ページのセクション **6.1.1** を参照してください。

5.3. ファイルシステムのウイルス保護

kavscanner コンポーネントは、サーバのファイルシステムをウイルスから保護します。このコンポーネントは、サーバファイルのウイルスをスキャンし、感染オブジェクトや感染の疑いがあるオブジェクトを設定に従って処理します。

処理方法としては、単に通知を行うだけ(レポートおよびサーバコンソールや管理者に送信された情報)、またはオブジェクトに変更を加える(駆除、隔離、削除を行う)こともできます。

kavscanner コンポーネントの設定は、すべて *kav4mailservers.conf* 設定ファイルの**[scanner.*]**オプション内にグループ化されています。

サーバファイルシステムのオンデマンドスキャンは、コマンドラインから起動するか標準の **cron** ユーティリティを使用してスケジュールできます。ファイルシステムのスキャン対象範囲は、ファイルシステム全体から特定のディレクトリやファイルまで指定できます。

以下のセクションでは、サーバファイルシステムのウイルス保護の最も一般的なタスクについて説明します。

サーバ全体のウイルススキャン処理は、大量のリソースを消費します。サーバ全体のスキャン中は、サーバの全体的なパフォーマンスが低下するため、他の処理を同時に実行することはお奨めできません。そうならないようにするために、ディレクトリを個々にスキャンすることをお奨めします。

5.3.1. オンデマンドスキャン

Kaspersky Anti-Virus では、指定したサーバディレクトリ内のファイルをスキャンおよび駆除することができます。

行うこと：**/tmp** ディレクトリのスキャンを再帰的に開始します。感染オブジェクトはすべて自動的に駆除するようにします。駆除できないオブジェクトは削除します。

コンポーネントアクティビティの結果(開始日、ウイルスが含まれていないファイル以外のすべてのファイルに関する詳細な情報)を、同一ディレクトリ内の *kavscanner-<current_date>-pid.log* というレポートファイルに保存します。

方法：このタスクを完了するには、コマンドラインに以下のコマンドを入力します。

```
-Rlq
-okavscanner-`date +%F`.log
```

スキャン処理でアーカイブ内に感染オブジェクトが検出された場合は、そのアーカイブ全体が削除されます。

5.3.2. ディレクトリを毎日自動的にスキャンする (cron)

標準的な Unix のスケジューリングユーティリティである **cron** を使用して、指定したディレクトリを定期的にスキャンするなど、Kaspersky Anti-Virus のタスクを自動で行うことができます。

行うこと：ウイルススキャンが毎日 0 時 0 分に**/home** ディレクトリで開始されるようスケジューリングを設定します。*/etc/kav/kavscanner.conf* 設定ファイルに定義されているスキャンパラメータを使用します。

方法：このタスクを完了するには、以下の手順を実行します。

1. 必要なスキャンパラメータがすべて含まれている */etc/kav/kavscanner.cron* 設定ファイルを作成します。
2. コマンドラインで **crontab –e** と入力することにより、**cron** 処理のタスクを設定するファイルを変更し、以下の内容を追加します。

   0 0 * * * /path/to/kavscanner -c /etc/kav/kavscanner.cron /home

5.3.3. 高度なオプション：スクリプトファイルの使用

Kaspersky Anti-Virus では、標準的な Unix/Linux コマンドおよびスクリプトファイルを使用して、ウイルス解析が完了したオブジェクトをさらに処理することができます。経験を積んだ管理者は、これらのツールを使用して、さまざまな状態のオブジェクトに適用されるさまざまな動作を定義することにより、Kaspersky Anti-Virus の機能を拡張できます。

5.3.3.1. アーカイブ内の感染オブジェクトの駆除

アーカイブをスキャンするには、アーカイブを操作するためのアーカイバがインストールされている必要があります。

Kaspersky Anti-Virus は、圧縮された感染ファイルの駆除は行いません。アーカイブ内の感染オブジェクトや感染の疑いがあるオブジェクトの検出のみ行います。ただし、*tar*、*rar*、*tgz*、および *zip* アーカイブを駆除するための *vox.sh* スクリプトなどの追加スクリプトを使用することにより、圧縮されたファイルを駆

除することができます。このスクリプトは、Kaspersky Anti-Virus の配布パッケージに含まれています。

行うこと：サーバ上のアクセス可能なすべての *tar* および *zip* アーカイブをスキャンし、*vox.sh* スクリプトを使用して、アーカイブ内のすべての感染オブジェクトを駆除します。/etc/kav/*kavscanner.conf.in* を設定ファイルとして使用します。スキャンを開始する前に、このファイルで、アーカイブを駆除するためのスクリプトアプリケーションを指定する必要があります。

すべての感染オブジェクトを完全パスと共に*/tmp/infected_archive.lst* ファイルにリストします。コンポーネントアクティビティのレポートを*/tmp/logfile.log* ファイルに保存します。

方法：このタスクを完了するには、以下の手順を実行します。

1. 代わりに使用する *kavscanner.conf.in* ファイルを作成します。
2. 感染オブジェクトを処理するためのルールを定義するために、設定ファイルの**[scanner.container]**セクションに以下の内容を追加します。

   ```
   OnInfected=exec
   /opt/kav/5.5/kav4mailservers./contrib/vox.sh %FULLPATH%/%FILENAME%
   ```

3. コマンドラインで、以下のコマンドを入力します。

   ```
   # kavscanner –c kavscanner.conf.in –ePASE –qR –o /tmp/logfile.log –j3 –pi/tmp/infected_archive.lst /
   ```

5.3.3.2. 管理者への電子メール通知

Kaspersky Anti-Virus では、標準的な Unix/Linux ツールを使用して、サーバファイルシステム内で検出された感染オブジェクト、感染の疑いがあるオブジェクト、または破損オブジェクトについて、管理者に通知するよう設定できます。

行うこと：アプリケーション設定ファイルで定義されているパラメータに基づいてサーバスキャンが実行される際に、サーバファイルシステム内で検出された感染ファイルおよびアーカイブについて管理者に知らせるための通知を設定します。

方法：このタスクを完了するには、以下の手順を実行します。

アプリケーション設定ファイルで、シンプルオブジェクトおよびコンテナオブジェクトを処理するためのルールを定義します。

[scanner.object]

OnInfected=exec echo %FULLPATH%/%FILENAME% is infected by %VIRUSNAME% | mail -s kavscanner admin@localhost.ru

[scanner.container]

OnInfected=exec echo archive %FULLPATH%/%FILENAME% is infected, viruses list is in the attached file %LIST% | mail -s kavscanner -a %LIST% admin@localhost.ru

5.3.4. 別のディレクトリにオブジェクトを移動する (隔離)

サーバファイルシステム内で検出されたすべての感染オブジェクトを特別なディレクトリに移動するよう Kaspersky Anti-Virus を設定することができます。
たとえば、ディレクトリのウイルススキャンにおいて、重要なデータが含まれている感染ファイルが検出された場合などに、この方法を使用します。駆除する際にデータの一部が失われる可能性があるため、このような場合は、感染オブジェクトを特別なディレクトリにいったん隔離してから、カスペルスキーラブスに送信して分析を依頼するなどの処置をとることが適切です。
サーバのファイルシステム内に Quarantine（隔離）ディレクトリを作成する場合は、アプリケーション設定ファイルの **ExcludeDir** パラメータでこのディレクトリの完全パスを指定することにより、このディレクトリを後続のスキャンの対象範囲から外すことをお奨めします。

行うこと：*/tmp/download.lst* ファイルにリストされているすべてのオブジェクトをスキャンし、感染オブジェクトがある場合は、それを完全パスと共に*/tmp/infected* ディレクトリに移動します。ヒューリスティックコード解析を使用します。再帰的なスキャンを無効にします。感染オブジェクト、感染の疑いがあるオブジェクト、および破損オブジェクトに関する情報をレポートファイルに記録します。

方法：このタスクを完了するには、以下の手順を実行します。

1. 感染オブジェクトの処理方法を定義するために、設定ファイルの **[scanner.object]**および**[scanner.container]**セクションに以下の内

容を追加します。

OnInfected=movePath /tmp/infected

2. 駆除モードが有効になっている場合は無効にします(**Cure=no**)。
3. コマンドラインで、以下のコマンドを入力します。

#kavscanner –@/tmp/download.lst –ePASBME –rq –i0 -o /tmp/report.log –j3 –mCn

/tmp/infected ディレクトリ内のファイルのアクセスを、読み取りおよび書き込みのみに制限する必要がある場合は、標準的な Unix ツール(**chmod** コマンド)を使用して、タスク構造に以下の変更を加えます。

感染ファイルを処理するためのルールとして、アプリケーション設定ファイルの**[scanner.object]**および**[scanner.container]**セクションに以下の内容を追加します。

OnInfected=exec mv %FULLPATH%/%FILENAME% /tmp/infected/%FILENAME%; chmod –x /tmp/infected/%FILENAME%

5.3.5. 処理対象オブジェクトのバックアップ

感染ファイルのデフォルト動作として、ファイルが自動的に削除されるよう設定されている場合、必要なデータが失われる可能性があります。また、駆除処理中にはデータが危険にさらされます。それを避けるために、Kaspersky Anti-Virus には、感染ファイルをバックアップ保存ディレクトリにコピーする機能があります。各オブジェクトの完全パスも記録されるため、必要に応じて後から元に戻すことができます。

オブジェクトを駆除または削除する前に、**[scanner.path]**セクションの **BackupPath** パラメータで指定されているバックアップ保存ディレクトリに、オブジェクトを自動的にコピーするようアプリケーションを設定できます。バックアップ保存ディレクトリに同一ファイルが記録される場合、以前にコピーされたファイルが、新しいファイルに自動的に置き換えられます。

デフォルトでは、このバックアップモードはオフになっているため、バックアップ保存ディレクトリのパスは定義されていません。したがって、バックアップモードを有効にするには、設定ファイルでこのパスを指定する必要があります。

ファイルシステムからオブジェクトが削除された場合、そのバックアップファイルは、管理者が削除しない限り保存されます。

5.4. ライセンスキーの管理

ライセンスキーは、アプリケーションを使用する権利を与えます。また、ライセンスキーには、ライセンスタイプ、有効期限、保護ユーザ数またはライセンスされたトラフィック量(ライセンスタイプによって異なる)、および販売元に関する情報などのライセンスに関するデータが含まれています。
ライセンスの有効期間中は、以下のサービスを受けることができます。

- 24 時間対応の技術サポート
- ウイルス定義データベースの毎時更新
- アプリケーションの更新(パッチ)
- アプリケーションの新規バージョン(アップグレード)
- 新しいウイルスに関する通知

ライセンスの有効期限が切れると、これらのサービスは自動的に打ち切られます。Kaspersky Anti-Virus でサーバファイルシステムおよびメールトラフィックのスキャンを継続して行うことはできますが、ウイルス定義データベースの更新機能が利用できなくなるため、ライセンスの期限が切れた時点のウイルス定義データベースしか使用できません。ライセンスの期限切れについては、管理者に通知されます。
したがって、ライセンスキーの情報を定期的に確認し、ライセンスを適宜更新する必要があります。

5.4.1. ライセンスのメカニズム

Kaspersky Anti-Virus 5.5 では、新しいライセンス技術が使用されています。サーバでのインストール中に、アプリケーションによる電子メールスキャンの対象となるドメインのリストを管理者が指定する必要があります。ライセンスは、以下に対して発行されます。

- 一定量のスキャントラフィック
- 一定数の保護対象ユーザアカウント

前者の場合、ライセンストラフィックには、アプリケーションが受信、スキャン、および **Clean** ステータス(ウイルスが含まれていない状態)の割り当てを行ったメッセージの総量が含まれます。
後者の場合、アプリケーションによってスキャンおよび処理される非感染メッ

セージの送信者および受信者が、ライセンスユーザとしてみなされます。
アプリケーションにより、ライセンス有効期限の 14 日前に管理者に通知が行われます。この通知は、24 時間ごとに 1 回と、アプリケーションの起動時に送信されます。
電子メールトラフィックがライセンストラフィック量を超えた場合にも、ライセンスの期限切れの場合と同じ通知が送信されます。
ただし、超過トラフィック量がライセンストラフィック量の 10%を超えると、ステータスが **Clean** 以外のメッセージが検出されるたびに、それに応じた通知が管理者に送信されます。

ライセンスメカニズムを正しく機能させるには、以下の操作を行う必要があります。

[smtpscan.license]セクションの **LicenseDomain** パラメータを定義します。このパラメータは、ライセンスユーザを含むドメインのマスク(POSIX regexp 規格に従う)を指定します。このパラメータの引数には、Kaspersky Anti-Virus によって保護されるすべてのメールドメインを含める必要があります。ドメイン名は、POSIX regexp 形式で、単一行にカンマで区切って指定します。

POSIX regexp 形式では「.」に独自の意味があるため、「.」を「\」で挟んで入力してください。

5.4.2. ライセンスキー情報の表示

インストールされているライセンスキーの情報は、*kavscanner*、*kavmonitor*、および *keepup2date* コンポーネントによって生成されるログ内で確認することができます。これらのコンポーネントは、起動時にライセンスキーから情報をロードします。
さらに、Kaspersky Anti-Virus には特別な *licensemanager* コンポーネントが含まれています。このコンポーネントを使用すると、分析データと共にキーに関する詳細情報を確認することができます。
たとえば、メールトラフィック量に基づくライセンス付きの Kaspersky Anti-Virus を購入した場合、*licensemanager* コンポーネントを使用すると、使用されたトラフィック量を把握することができ、ライセンスメールトラフィック量の残量(Mb 単位)が通知されます。
また、その日に処理されたトラフィック量(時間単位)に関する情報も確認できるため、ロード量がいつ最大量に達するかがわかります。これらの情報は、アプリケーションで問題が発生して技術サポートに問い合わせる必要がある場合などに役立ちます。

ユーザ数に基づくライセンス付きのアプリケーションを購入した場合は、購入したライセンスに含まれるライセンスユーザの総数を確認できます。
これらの情報は、すべてサーバのコンソールに出力できます。

インストールされているすべてのライセンスキーに関する情報を表示するには、以下の操作を実行します。

コマンドラインで、以下のコマンドを入力します。

licensemanager –s

インストールされているライセンスに関する情報が、以下のような様式でサーバのコンソールに出力されます。

Kaspersky license manager Version 5.5

Copyright (C) Kaspersky Lab. 1998-2005.

License file 0003D3EA.key, serial 0038-000419-0003D3EA, "Kaspersky Anti-Virus for Unix Mail Servers", expires 04-07-2003 in 28 days

License file 0003E3E8.key, serial 011E-000413-0003E3E8, "Kaspersky Anti-Virus for Unix Mail Servers (licence per e-mail address)", expires 25-01-2004 in 234 days

特定のライセンスキーに関する情報を表示するには、以下の操作を実行します。

たとえば、コマンドラインで、以下のようなコマンドを入力します。

licensemanager –k 0003D3EA.key

以下のような様式でコンソールに情報が出力されます。

Kaspersky license manager Version 5.5

Copyright (C) Kaspersky Lab. 1998-2005.

Serial 0038-000419-0003D3EA, "Kaspersky Anti-Virus for Unix Mail Servers", expires 04-07-2003 in 28 days

ライセンスメールトラフィックまたは保護ユーザ数に関する情報を表示するには、以下の操作を実行します。

コマンドラインで、以下のコマンドを入力します。

licensemanager –i

以下のような様式でサーバのコンソールに情報が出力されます。

- *ユーザ数*に基づくライセンスの場合：

  Kaspersky license manager for Linux. Version 5.5.0/RELEASE #68
  Copyright (C) Kaspersky Lab, 1997-2005.

Portions Copyright (C) Lan Crypto

License users units: 5
Users units used: 0
Users units left: 5

- *メールトラフィック量*に基づくライセンスの場合：

  Kaspersky license manager Version 5.5
  Copyright (C) Kaspersky Lab. 1998-2005.
  Daily traffic statistic(Bytes):
  0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
  License traffic units: 10 (MB)
  Traffic units used: 0 (MB)
  Traffic units left: 10 (MB)

5.4.3. ライセンスの更新

Kaspersky Anti-Virus を使用するためのライセンスを継続すると、ウイルス定義データベースの更新や 53 ページのセクション **5.3.5** に記載されているその他のサービスを含むアプリケーションのすべての機能が続行または回復します。

Kaspersky Anti-Virus を使用するためのライセンスを継続するには、以下の作業を行う必要があります。

アプリケーションの販売元から、Kaspersky Anti-Virus を使用するための継続ライセンスを入手します。

新しいライセンスキーは、インストールする必要があります。インストールするには、設定ファイルの**[path]**セクションの **LicensePath** パラメータで指定されているキー保管用ディレクトリにライセンスキーをコピーします。その後、サーバを再起動します。
再起動したら、すぐにウイルス定義データベースを更新することをお奨めします(34 ページのセクション **5.1** を参照)。

第6章 高度な設定

このセクションでは、Kaspersky Anti-Virus の機能の高度な設定について説明します。インストール処理中に設定される、製品の使用に不可欠な必須設定(25 ページの**第 4 章**を参照)と違って、高度な設定は、管理者の判断で使用できます。高度な設定は、アプリケーションの機能を拡張し、特定の業務要件を満たすよう調整するために使用します。

6.1. メールトラフィックのウイルス保護の設定

メールトラフィックのウイルスをスキャンする場合、各メールメッセージの処理ルールは、送信者および受信者のアドレスと、それらが属するグループのパラメータに基づいて選択されます。したがって、アドレスを適切なグループに作成することが非常に重要です。

メッセージが特定のグループに属するかどうかは、送信者と受信者の両方のアドレスがそのグループに存在するかどうかで判断されます。プログラムは、グループのアドレスリストで、それらの両方のアドレスを探します。分析対象のグループ内にこの 2 つのアドレスの組み合わせ(送信者と受信者)が存在する場合、このグループのルールに従ってメッセージが処理されます。

Kaspersky Anti-Virus は、*kav4mailservers.conf* 設定ファイルに指定されている設定に従って、アンチウイルスフィルタリングを実行します。このファイルは、ローカルで編集することはできません。

メッセージのアドレスがグループに存在するかどうかの確認は、**POSIX regex** に従って行われます(この規格の詳細については、『man 7 regex』を参照してください)。

デフォルトでは、メールメッセージの処理ルールを定義する**[smtpscan.group:default]**グループが設定ファイルに含まれています。このグループは、最初は送信者や受信者の名前が含まれていないため、このグループに指定されているルールは、すべてのメッセージに適用されます。**default** グループのパラメータを変更、または新しいグループを作成することができます。

設定ファイルに他のグループが追加されると(60 ページのセクション **6.1.1** を参照)、メールメッセージの処理手順は以下のようになります。

1. プログラムは、メッセージのアドレスが、管理者によって定義されたグループに属するかどうかをチェックします。メッセージのアドレスがユーザアドレスグループに属する場合、このグループのルー

ルに従ってメッセージが処理されます。

メッセージの送信者および受信者のアドレスが複数のグループに存在する場合は、最初に検出されたグループのパラメータが使用されます。

2. これらのアドレスが、管理者によって定義されたどのアドレスグループにも属さない場合は、**default** グループに指定されているルールに従ってメッセージが処理されます。

図 5 は、Kaspersky Anti-Virus による受信メールメッセージの処理手順を示しています。

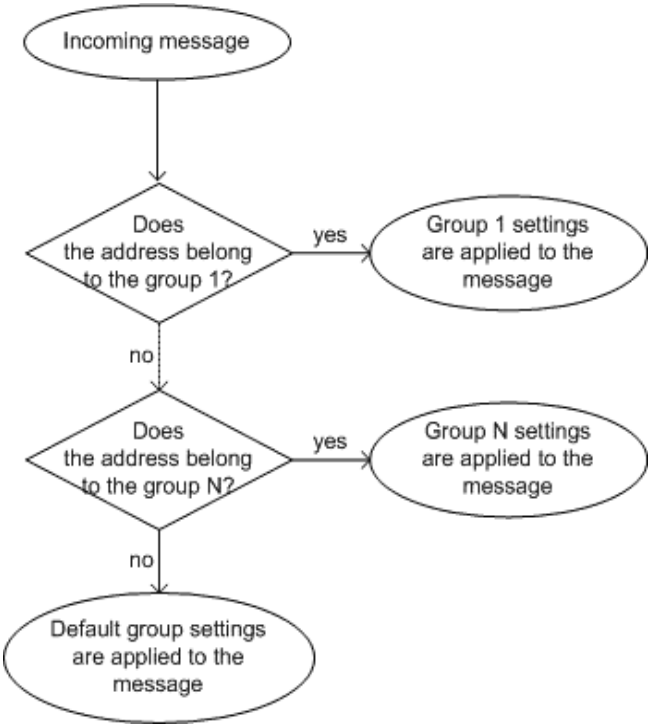

図 5. メールメッセージの処理

6.1.1. ユーザグループの作成

デフォルトでは、Kaspersky Anti-Virus の設定ファイルには、サーバのすべての送受信者を含む**[smtpscan.group:default]**グループが含まれています。このグループでは、以下のルールを使用してメールメッセージが処理されます。

- すべてのメッセージをチェックします。
- 検出されたすべての感染ファイルを駆除します。
- 感染していないメッセージと駆除済みメールメッセージのみ配信します。
- 駆除できないメッセージ、感染の疑いがあるメッセージ、破損メッセージ、パスワードで保護されたメッセージ、およびスキャンできないメッセージは、グループ管理者にのみ配信されます。
- 感染メッセージ、駆除されたメッセージ、感染の疑いがあるメッセージ、破損メッセージ、パスワードで保護されたメッセージ、およびスキャンできないメッセージについて、送信者、受信者、およびグループ管理者に通知します。

Kaspersky Anti-Virus を使用して、送受信者に応じたさまざまなルールを使用してメールメッセージを処理したい場合は、グループを作成する必要があります。

新しいユーザグループを作成するには、以下の手順を実行します。

1. 設定ファイル内に**[smtpscan.group:<group_name>]**セクションを作成します。
2. グループに含める受信者および送信者のアドレスまたはアドレスマスクを定義します。これらを定義するには、**Senders** および **Recipients** パラメータの値として、これらをカンマで区切ってリストします。

POSIX regex 規格に従ってマスクをリストします。2つ以上のマスクを使用する場合は、それらをカンマで区切ります。

Recipients または **Senders** パラメータのいずれかの値が定義されていない場合、自動的に「**.*@.***」が設定されます。

Kaspersky Anti-Virus バージョン 5.5 では、設定ファイルに **kavadministrators** グループが導入されています。アプリケーションのセットアップ中に、/var/qmail/alias/postmaster ディレクトリにリストされている管理者の電子メールアドレスが、このグループに自動的に追加されます。

セットアップ後に管理者アドレスを変更する場合は (**[smtpscan.group:default]** またはその他のグループの **AdminAddress** パラメータ)、新しい管理者アドレスとこのアドレスをエイリアスとして使用しているその他のアドレスを **[smtpscan.group:kavadministrators]** グループの **Recipients** パラメータのリストに追加する必要があります。

感染メールメッセージを管理者に配信するよう設定している場合、これは重要な作業です。

6.1.2. メッセージのチェックおよび駆除モード

特定の送受信者グループのメールトラフィックをスキャンしてウイルスチェックするには、サーバの管理者が、そのグループのパラメータで該当するモードを有効にする必要があります。
有効にするには、*kav4mailservers.conf* 設定ファイルで、対応するグループに **Check=yes** パラメータを設定します。
Check モードを有効にすると、送受信者に基づいてそのグループに属すると判断されるすべてのメールメッセージが、Kaspersky Anti-Virus によってスキャンされ、ウイルスチェックされます。ただし、感染メールメッセージの駆除は行われません。
感染メッセージの*駆除モードを有効にするには*、そのグループで**駆除済み**オブジェクトに関するパラメータを 1 つ以上指定する必要があります。たとえば、グループの他のパラメータと共に以下のパラメータを指定します。

```
[smtpscan.group:account]
Check=yes
CuredRecipientNotify=yes
```

その場合、以下のように処理されます。

- **account** グループに含まれる送受信者のすべてのメールメッセージのウイルスチェックが行われます。
- 感染オブジェクトが検出された場合は駆除されます。
- 駆除されたオブジェクトについての通知が受信者に送信されます。

6.1.3. メールメッセージに関する動作

以下の 2 つの要素により、メールメッセージに適用される動作が決定されます。

- スキャン後に割り当てられるオブジェクトのステータス(69 ページのセクション **6.3.2** を参照)
- 設定ファイルで特定のオブジェクトに指定されている動作

オブジェクトのステータスは、ウイルススキャン直後に *aveserver* 処理によって割り当てられます。スキャン後に適用される動作は、サーバの管理者が設定します。

Kaspersky Anti-Virus®では、受信者およびグループ管理者に配信されるメールオブジェクトに適用する動作を指定できます。メッセージの送信者には、通知のみ送信できます。

以下の動作をメールメッセージオブジェクトに適用できます。

Remove – メッセージからオブジェクトを削除します。

Unchanged – オブジェクトをそのまま配信します。この場合、オブジェクトが駆除されず、元の形のまま配信されます。

Cured – 感染していないオブジェクトまたは駆除済みのオブジェクトのみ配信されます。

*共通動作*をすべてのオブジェクト形式に設定したり、形式ごとに指定したりできます。

すべてのオブジェクト形式に共通の動作を適用するには、以下の手順を実行します。

AdminAction および **RecipientAction** パラメータに、適用する値を設定します。これらのパラメータは、すべてのオブジェクト形式に適用される動作を定義するパラメータです。たとえば、以下のように設定します。

```
AdminAction=unchanged
RecipientAction=remove
```

この場合、グループのすべてのメールメッセージの添付ファイルがそのまま管理者に配信されますが、受信者のメッセージからは削除されます。

オブジェクト形式ごとに動作を設定するには、以下の手順を実行します。

<object_type>AdminAction および**<object_type>RecipientAction** パラメータに、適用する値を指定します。

たとえば、以下のように設定します。

AdminAction=unchanged
RecipientAction=remove
CuredRecipientAction=cured

この場合、オブジェクト形式に関係なくすべてのメールメッセージがそのままグループ管理者に配信されますが、受信者には駆除済みのメッセージのみ配信されます。その他の形式のオブジェクトは、メールメッセージから削除されます。

上記の動作の他に、**隔離ディレクトリにオブジェクトを移動することもできます。**

メールメッセージオブジェクトを隔離ディレクトリに移動するには、以下の手順を実行します。

グループ設定ファイルで、以下のパラメータを設定します。

QuarantinePath=/var/db/Quarantine
Quarantine=yes
SuspiciousQuarantine=yes
CorruptedQuarantine=yes
ErrorQuarantine=yes

送信者、受信者、および管理者への通知

Kaspersky Anti-Virus では、すべてのステータス(感染の疑いがある、感染している、駆除済み、破損している、など)のオブジェクトについて、メールメッセージの送信者、受信者、およびグループ管理者に送信される通知(配信モード、生成パラメータ、およびテキストなどを含む)を設定することができます。**通知の送信方法**は、以下の設定パラメータで制御します。

- **RecipientNotify** – メールメッセージの受信者に通知を送信します。
- **SenderNotify** – メールメッセージの送信者に通知を送信します。

- **AdminNotify** – グループ管理者に通知を送信します。

これらのパラメータは、ステータスに関わらず、オブジェクトに関する通知の送信方法を定義します。特定のステータスのオブジェクトについて通知を送信するよう設定するには、以下のモードを有効にします。

- **<object_status>RecipientNotify**
- **<object_status>SenderNotify**
- **<object_status>AdminNotify**.

この場合、指定されたステータスのオブジェクトに関してのみ通知が送信されます。
たとえば、グループで以下のような設定を指定できます。

InfectedRecipientNotify=yes
CuredRecipientNotify=yes
CorruptedRecipientNotify=yes
SenderNotify=yes
AdminNotify=yes

この場合、管理者と送信者には、すべてのステータスのオブジェクトに関する通知が送信され、受信者には、感染オブジェクト、駆除済みオブジェクト、および破損オブジェクトに関する通知のみ送信されます。
通知を送信するには、送信元のアドレスも指定する必要があります(**[smtpscan.general]**セクションの **NotifyFromAddress** パラメータ)。
デフォルトでは、すべてのステータスのオブジェクトに関する通知が有効になっています。これらの通知には、配布キットに含まれている */etc/kav/5.0/template_notify_main* テンプレートに基づいた**一般的なテキスト**が含まれます。
通知のテキストを編集したい場合は、以下のいずれかの方法で編集できます。

- プログラムで用意されているテキストを編集します。
- 新しいテンプレートファイルを作成し、そのファイルの完全パスを **[smtpscan.notify]**セクションの **Template** パラメータの値として指定します。

テンプレートのテキストでは、以下のマクロを使用できます。これらのマクロは、*aveserver* 処理の結果に応じて対応する値に置き換えられます。

%VERSION% – Kaspersky Anti-Virus のバージョン
%SENDER% – メッセージの送信者のアドレス

%RECIPIENT% – メッセージのすべての受信者のリスト(改行文字で区切られる)

%MSGID% – メッセージの ID 番号

%VIRUSNAME% – 問題を説明するテキスト。すべてのステータスのオブジェクトについて、**[locale]**セクションに対応する内容を入力することにより、このテキストを任意の言語に変換できます。

%SUBJECT% – 元のメールメッセージの件名フィールドの内容を挿入します。

%DATETIME% – メッセージの処理日時。時間および日付の表示形式も編集できます。

%HEADERS% – 元のメッセージのすべてのヘッダがテキストに追加されます。

%ACTION% – 添付オブジェクトに適用される動作の記述。メッセージの送信者への通知以外のすべてのテンプレートでマクロを使用できます。以下の動作を設定できます。

attachement not modified – 添付オブジェクトはそのままの状態です。

attachement cured – 添付オブジェクトが感染していましたが、駆除に成功しました。

attachment removed – 添付オブジェクトが削除されました。

attachments cured and removed – 添付オブジェクトが感染していました。一部は駆除されて受信者に配信され、一部は削除されました。

メッセージの件名を作成する際にもこれらのオブジェクトを使用できます。
通知生成パラメータ(MIME 形式、件名、コードページなど)は、設定ファイルの**[smtpscan.notify]**セクションにグループ化して指定します。

6.2. Postfix 用の追加機能

Kaspersky Anti-Virus を Postfix 電子メールシステムと共に使用する場合、さまざまな追加機能を使用できます。

- DSN SMTP 拡張のサポート(RFC 3461、RFC 3885) (66 ページのセクション **6.2.1** を参照)
- 8bit-MIME SMTP 拡張のサポート(RFC 1652) (66 ページのセクション **6.2.2** を参照)

- X-Forward SMTP 拡張のサポート(67 ページのセクション **6.2.3** を参照)

これらの技術は、管理者の判断で設定できます。以下のセクションでは、これらについて詳しく説明します。

6.2.1. DSN 拡張のサポート

smtpscanner コンポーネントは、SMTP プロトコルの DSN 拡張をサポートします。DSN 拡張を使用することにより、受信メールシステムによって後続のシステムに割り当てられるメールメッセージのパラメータが、コンポーネントによって維持されます。この場合、smtpscanner はパラメータを分析せず、代わりにそのままルーティングメールシステムに転送します。

DSN のサポートを有効にするには、以下の手順を実行します。

アプリケーション設定ファイルの**[smtpscan.general]**セクションで、以下のパラメータを定義します。

EHLOsupportDSN=yes

オプションを有効にする前に、ルーティングメールシステムが DSN 拡張をサポートしていることを確認してください。

6.2.2. 8bit-MIME 拡張のサポート

メールシステムが、SMTP を使用して国別エンコードを行う場合、8bit-MIME がよく使用されます。そのため、Kaspersky Anti-Virus 5.5 では、この拡張のサポートが追加されました。

使用している外部メールシステムが 8bit-MIME 拡張をサポートしていない場合は、Kaspersky Anti-Virus の設定でもこの拡張を無効にする必要があります。

8bit-MIME のサポートを有効にするには、以下の手順を実行します。

アプリケーション設定ファイルの**[smtpscan.general]**セクションで、以下のパラメータを定義します。

EHLOsupport8BITMIME=yes

Kaspersky Anti-Virus は、この拡張のサポートが有効でも無効でも、ウイルスやその他の悪意のあるオブジェクトからサーバを保護します。

6.2.3. X-Forward 拡張のサポート

Kaspersky Anti-Virus の運用では、Postfix プロトコル用の X-Forward 拡張がサポートされます。

X-Forward のサポートを有効にするには、以下の手順を実行します。

- Anti-Virus が Postfix と統合されている場合は、SMTP プロトコルを使用します(詳細については、34 ページのセクション **4.4.5** を参照)。
- アプリケーション設定ファイルの**[smtpscan.general]**セクションで、以下のパラメータを定義します。

  EHLOsupportXFORWARD=yes
  EHLOattrsXFORWARD=NAME ADDR PROTO HELO

6.2.4. 受信 SMTP のサポート

smtpscanner コンポーネントは、LMTP または SMTP を使用してトラフィックを受信することができます。

smtpscanner の SMTP サポートを有効にするには、以下の手順を実行します。

- Kaspersky Anti-Virus をサーバにインストールします。
- **LMTP** 経由の統合を含む、インストール後の設定を実行します(詳細については、34 ページのセクション **4.4.5** を参照)。
- アプリケーション設定ファイルの**[smtpscan.general]**セクションで、**Protocol** パラメータに **smtp** を割り当てます。
- Postfix 設定ファイル*(master.cf)*の smtp サービスの設定で、プロトコルの値を lmtp から smtp に変更します。
- メールシステムを再起動します。

6.3. サーバファイルシステムのウイルス保護の設定

サーバファイルシステムを保護するためのパラメータは、以下の設定内容に応

じてグループ分けされています。

- スキャン範囲(68 ページのセクション **6.3.1** を参照)
- ファイルのスキャンおよび駆除モード(69 ページのセクション **6.3.2** を参照)
- ファイルの操作(70 ページのセクション **6.3.3** を参照)
- アプリケーションアクティビティのレポート用のパラメータ(75 ページのセクション **6.6** を参照)

以下のセクションで、これらの各グループの設定について説明します。

6.3.1. スキャン範囲

スキャン範囲は、以下の 2 つの要素に分けられます。

- *スキャンパス*は、ウイルススキャンの対象ディレクトリおよびファイルのリストです。
- *スキャンオブジェクト*は、ウイルススキャンを行うファイルの形式です(アーカイブ、電子メールメッセージ、など)。

デフォルトでは、ファイルシステムのアクセス可能なすべてのオブジェクトのスキャンが、現在のディレクトリから開始されます。

サーバファイルシステム全体をスキャンするには、コマンドラインでスキャン範囲として最初にルートを入力するか、「**/**」を指定します。

スキャンパスは、以下の方法で再定義できます。

- コンポーネントの起動時に、絶対パスまたは相対パス(現在のディレクトリへの)と共にディレクトリおよびファイルを、コマンドラインにスペースで区切って列挙します。
- テキストファイル内にスキャンパスを定義し、コマンドラインオプションの**-@ <file_name>**を使用して、このファイルを使用するコマンドを発行します。ファイル内の各オブジェクトが、絶対パスと共に新しい行としてリストに追加されます。

スキャンパスと、スキャン対象オブジェクトのリストを含むテキストファイルの両方がコマンドラインに含まれている場合、テキストファイル内にリストされたオブジェクトのみ処理されます。コマンドラインで指定されているパスは無視されます。

- デフォルトパス(すべて現在のディレクトリから開始される)やコマンドラインにリストされたパスを制限するには、スキャン範囲から除外するファイルおよびディレクトリのマスクを入力します。設定ファイルの **[scanner.options]**セクションの **ExcludeMask** および **ExcludeDirs** パラメータを使用します。
- *ディレクトリの再帰的なスキャン*を無効にします(**[scanner.options]**セクションの **Recursion** パラメータまたは**–r** キー)。
- 代替設定ファイルを作成し、コンポーネントの起動時に、コマンドラインオプションの**– c <file_name>**を指定してこのファイルを使用します。

デフォルトのスキャンオブジェクトも *kav4mailservers.conf* 設定ファイル(**[scanner.options]**セクション)で指定されており、以下の方法で再定義することができます。

- 設定ファイル内で直接定義します。
- コンポーネントの起動時に、コマンドラインオプションを使用します。
- 代替設定ファイルを使用します。

6.3.2. ファイルのスキャンおよび駆除モード

これらの設定により、アプリケーションが感染ファイルの駆除を行うかどうかが決まるため、スキャンを行う際はこれらのモードを設定する必要があります。デフォルトでは、駆除オプションは無効になっています。つまり、スキャン処理では、ウイルス感染オブジェクト、感染の疑いがあるオブジェクト、または破損オブジェクトが検出されたことを知らせるメッセージが、コンソールおよびレポートに送信されます(75 ページのセクション **6.6** を参照)。
スキャン処理の結果、各オブジェクトに以下のいずれかのステータス値が割り当てられます。

- **Clean** – ウイルスは検出されませんでした。
- **Infected** – このファイルは感染しています。
- **Warning** – このファイルのコードは、既知のウイルスに類似しています。
- **Suspicious** – このファイルは、未知のウイルスに感染している疑いがあります。
- **Corrupted** – このファイルは破損しています。

- **Protected** – このファイルはパスワードで保護されているため、スキャンできません。

駆除モードが有効な場合(**[scanner.options]**セクションの **Cure=yes** パラメータ)、ステータスが **Infected** のファイルのみアンチウイルス処理に送られます。駆除後のファイルには、以下のいずれかのステータスが割り当てられます。

- **Cured** – このファイルは、駆除に成功しました。
- **CureFailed** – ファイルの駆除に失敗しました。これらのファイルは、感染オブジェクト用に定義されているルールに従って処理されます。

6.3.3. 感染の疑いがあるファイルおよび感染ファイルに適用する操作

ステータスに応じて、ファイルに特定の動作を適用できます(69 ページのセクション **6.3.2** を参照)。デフォルトでは、確実に感染しているファイルが検出された場合のみ、通知が送信されます。その場合の通知メッセージは、コンソールおよびレポートに出力されます。
ただし、ステータスが **Infected**、**Suspicious**、**Warning**、、**Corrupted** のファイルについては、以下のように動作を具体的に定義することもできます。

- *指定されたディレクトリに転送する* – 定義されているステータスのファイルを、指定されたディレクトリに移動します。*通常の転送*または*再帰的な転送*が可能です。
- ファイルシステムからファイルを*削除*します。
- *特定のコマンドを実行する* – 標準的な Unix コマンドやスクリプトなどを使用してファイルを処理します。

ステータスが **Protected** および **Cured** のファイルについては、コンソールおよびレポートに通知が出力されます。

Kaspersky Anti-Virus では、シンプルオブジェクト(ファイル)と複合オブジェクト(アーカイブなど、複数のオブジェクトで設定されるコンテナ)が区別されることに注意してください。これらの 2 種類のオブジェクトに適用される動作も区別されるため、設定ファイル内でも別々のセクションが割り当てられます。**[scanner.object]**セクションはシンプルオブジェクト用、**[scanner.container]**セクションは複合オブジェクト用です。

自己解凍アーカイブの場合、さまざまな操作が可能です。アーカイブ自体が感染している場合は、シンプルオブジェクトとして処理されますが、内部のアーカイブオブジェクトにウイルスが含まれている場合は、複合オブジェクトとして処理されます。アーカイブに適用されるこれらの 2 種類の操作は、それぞれ設定ファイルの異なるセクションのパラメータによって決定されるので注意してください。

以下の方法で、特定のファイルに適用する動作を選択することができます。

- デフォルト動作として使用する場合は、アプリケーション設定ファイル内に動作を指定します(**[scanner.object]**および**[scanner.container]**セクション)。
- 代替設定ファイルに動作を指定し、コンポーネントの起動時にそのファイルを使用します。
- *kavscanner* コンポーネントの起動時に、コマンドラインオプションを使用して、現在のセッションに適用する動作を定義します。

シンプルオブジェクトの場合もコンテナの場合も、動作を定義する構文は同じです。

6.3.4. バックアップモード

このセクションでは、以下のタスクを例に、バックアップモードの設定について説明します。

行うこと：*/tmp/download.lst*にリストされているディレクトリおよびファイル内のすべてのオブジェクトをウイルススキャンします。駆除できなかった場合、感染オブジェクトを完全パスと共に**/tmp/infected**ディレクトリに移動します。感染の疑いがあるオブジェクトは、**/tmp/suspicious**に移動し、通知を**/tmp/warning**に出力します。

方法：このタスクを完了するには、以下の手順を実行します。

1. 代替設定ファイルとして *scan_sample.conf* を作成します。
2. 感染オブジェクトの駆除モードを有効にします(**[scanner.options]** セクションの **Cure=yes**)。
3. 感染オブジェクトの処理ルールを設定します。設定するには、*scan_sample.conf* 設定ファイルの **[scanner.object]** および **[scanner.container]**セクションに以下の設定を追加します。

   OnInfected=MovePath /tmp/infected

OnSuspicion=MovePath /tmp/suspicious
OnWarning=MovePath /tmp/warning

4. コマンドラインで、以下のコマンドを入力します。

   # kavscanner -@/tmp/downloads.lst -c sample_scan.conf

6.4. Kaspersky Anti-Virus の最適化

Kaspersky Anti-Virus には、運用を最適化するための効率的な方法がいくつか用意されています。このセクションでは、それらの方法について詳しく説明します。

このセクションで説明する方法は、サーバファイルシステム内のオブジェクトをスキャンする際に使用する方法です。これらの使用は、アプリケーション設定ファイルの**[scanner.options]**セクションの対応するパラメータによって制御されます。

6.4.1. iChecker データベースの使用

最後のスキャン以降にファイルが変更されたかどうかをチェックすることにより、ファイルにアクセスするたびにスキャンしなおすのをやめることができます。この場合のオブジェクト(ファイル)のウイルススキャンアルゴリズムは、以下のようになります。

- ファイルの最初のスキャン後に、そのファイルに関する情報(ファイル名、チェックサム)が共通 iChecker データベースに追加されます。このデータベースには、*kavscanner* コンポーネントによってスキャンされた**感染していない**ファイルに関する情報が、指定された形式で格納されています。
- このファイルへの 2 回目以降のアクセスを行うと、まず iChecker データベースでファイル名が検索されます。ファイル名が検索条件として使用されます。iChecker データベース内にファイル名が見つかった場合、データベースに格納されているデータと現在の状態が比較されます。格納されている情報とファイルの現在の状態が完全に一致する場合、ファイルが変更されていないとみなされ、スキャンが実行されません。

iChecker データベースにもキャッシュにも当該ファイルの情報が見つからなかった場合は、ファイルのウイルススキャンが実行され、その結果がデータベースに更新されます。

6.4.2. サーバの負荷を軽減する

データ量の大きいサーバファイルシステムをスキャンする場合、かなりの時間がかかり、サーバの負荷が著しく増加する可能性があります。サーバでは、通常のタスクも実行する必要があるため、一定の負荷を超えた場合にウイルススキャンを一時的に停止できると便利です。
Kaspersky Anti-Virus バージョン 5.5 では、それが可能になりました。**[scanner.options]**セクションに **MaxLoadAvg** パラメータが追加されました。このパラメータが指定されている場合、*kavscanner* は、各ファイルのスキャンを開始する前に、現在のサーバの負荷(**load average** の値)を確認します。サーバの負荷が設定ファイルで指定されている量を超えている場合、指定されているしきい値まで **load average** の値が下がるまで、スキャン処理が一時停止されます。

6.5. *aveserver* 処理の設定

前述の通り、メールトラフィックのアンチウイルス処理は、2 つのコンポーネント(*aveserver* および *smtpscanner*)が相互にやり取りしながら実行されます。
aveserver は、オペレーティングシステムの起動時に起動されます。
smtpscanner が *aveserver* 処理にアクセスするとすぐに *aveserver* との接続が確立されます。
aveserver 処理は、*kav4mailservers.conf* 設定ファイルの**[aveserver.options]**セクションのパラメータによって制御されます。

Detach From Terminal – 起動直後に、ターミナルから処理の接続が切断されます。処理が切断されない限りシステムが起動されないため、このモードを有効にする必要があります。デフォルトでは、このモードは有効です(値は **yes**)。**SVC** などのプログラムによって処理が制御される場合のみ、このモードを無効にします(値は **no**)。

Startup Mode – **DetachFromTerminal=yes** の場合に、処理をダイアログモードからバックグラウンドモードに切り替えます。**fast** 値を指定すると、設定ファイルのロード直後に、コード **0** を返しながら、デーモンが処理をバックグラウンドモードに切り替えます。**normal** 値を指定すると、ウイルス定義データベースおよびライセンスキーがメモリにロードされてから、プロセスがバックグラウンドモードに切り替わります。

fast モードの方が速く起動されるように見えますが、何らかの致命的なエラーにより、デーモンがロードに失敗する可能性があります。その場合、コンソールには何も出力されません。

Local Socket Permission – ソケットのパーミッション(権限)を 8 進数で記述します。デフォルトでは、**Local Socket Permission=0666** です。

6.5.1. aveserver のリロード

aveserver 処理は、設定ファイルで対応する設定が有効になっている場合、ウイルス定義データベースの更新直後に自動的にリロードされます。
この処理は、**kill –HUP <process PID>**コマンドによってリロードされます。このコマンドの実行後、aveserver 処理が **SIGHUP** 信号を受信すると、親処理が設定ファイル、ライセンスキー、およびデータベースをリロードします。ファイルのパスが間違って設定されている場合は、処理が終了し、対応するメッセージがレポートに記録されます。この処理のクライアントプログラムとの接続は、プログラムが終了されるまですべてアクティブなまま維持されます。
たとえば、設定ファイルを編集したり、ライセンスキーを新しく追加したり、ウイルス定義データベースを手動で更新した後などに、aveserver 処理をリロードする必要があります。

6.5.2. aveserver 処理の強制終了

aveserver 処理を強制的に終了する必要がある場合は、**kill <process PID>**コマンドを使用します。kill コマンドは、処理に対して **SIGTERM** 信号を送信します。この信号により aveserver 処理が終了され、処理で作成されたすべてのコピーが閉じられます。

aveserver 処理の終了に **kill –9** コマンドを使用しないでください。このコマンドでも実際に処理が終了されますが、一時ファイルや作業ファイルがたくさん残ってしまい、手動で削除しなければならなくなります。一部のアプリケーション(Webmin など)は、これらのファイルを使用して、処理が実行中かどうかを検知します。

6.6. 日付および時刻の表示形式を地域に合わせる

Kaspersky Anti-Virus の作業では、各コンポーネントのレポートやユーザおよび管理者に送信される通知が作成されます。通常、これらには作成された日付および時刻が入ります。
デフォルトでは、Kaspersky Anti-Virus は、C 関数の strftime が使用する日付および時刻形式と一致する形式を使用します。

%H:%M:%S – 時刻の表示形式

%d/%m/%y – 日付の表示形式

管理者は、*kav4mailservers.conf* 設定ファイルの**[locale]**セクションのパラメータを使用して、日付および時刻の表示形式を変更できます。たとえば、以下のような形式を使用できます。

%I:%M:%S %P – am/pm 表示付きの 12 時間形式の時刻(**TimeFormat** パラメータ)

%y/%m/%d および **%m/%d/%y** – 年/月/日または月/日/年の形式の日付(**DateFormat** パラメータ)

6.7. Kaspersky Anti-Virus のレポート用パラメータ

Kaspersky Anti-Virus のすべてのコンポーネントによって実行された処理の結果は、レポートにまとめられて、ログファイルに出力されます。

サーバファイルシステムのアンチウイルス処理の結果もコンソールに出力されます。デフォルトでは、レポートに出力される情報とコンソールに出力される情報は同じ情報です。レポートログの情報と異なる情報をコンソールに表示するには、追加設定が必要です(詳細については、**6.7.2** セクションのページ 78 を参照)。

出力される情報量を変更するには、*レポート詳細レベル*を変更します。
詳細レベルは番号で表され、コンポーネントの作業に関する情報の冗長性レベルを設定します。番号が 1 つ大きくなると、前のレベルの情報にデータが追加されます。
指定可能なレポート詳細レベルを以下の表に示します。

レベル	レベル名	説明
	致命的なエラー	動作を実行できないためにプログラムが終了するような、重大なエラーに関する情報のみ。たとえば、アプリケーションコンポーネントが感染している場合や、スキャン、データベースのロード、またはライセンスキーのロードなどの重要な動作が失敗した場合などです。
1	エラー	その他のエラー(コンポーネントを終了させる原因にはならないエラー)に関する情報。ファイルをスキャンできない場合などです。
2	警告	アプリケーションが終了される可能性があるエラーに関する情報。空きディスクスペースが不十分な場合などです。
3	情報および通知	重要な情報。コンポーネントが実行されているかどうか、設定ファイルのパス、スキャン範囲、ウイルス定義データベースに関する情報、ライセンスキー、および統計情報などです。
4	動作内容	設定されているスキャンレポートの詳細レベルに応じたオブジェクトスキャンに関するメッセージ(77 ページのセクション **6.7.1** を参照)。
10	デバッグ	すべてのデバッグメッセージ。設定ファイルの内容などです。

コンポーネントの処理における致命的なエラーに関する情報は、選択されている詳細レベルに関わらず出力されます。デフォルト設定の **4** が、最適な詳細レベルです。

上記の詳細レベルに従って出力される情報は、一般に以下の形式で出力されます。

[date time level_of_detail] STRING

各コマンドおよびパラメータの意味は以下の通りです。

[date time level_of_detail]は、システムによって生成されるパラメータです。このパラメータは、日付と時刻(管理者が設定した形式で)およびレポートの詳細レベル(詳細レベルの先頭の文字)で設定されます。

日付と時刻の形式は、*kav4mailservers.conf* 設定ファイルの**[locale]**セクションで変更できます。

STRING – レポート行。メッセージの形式に応じて異なります。以下の

形式のメッセージがあります。

- スキャンに関するメッセージ(77 ページのセクション **6.7.1** を参照)
- その他のメッセージ(コンポーネントの起動、ウイルス定義データベースのロード、リターンコードなどに関するメッセージ)
- コンソールに出力されるメッセージ(78 ページのセクション **6.7.2** を参照)

以下のセクションでは、各メッセージ形式および形式について詳しく説明します。

6.7.1. スキャンに関するメッセージの形式

スキャンに関するメッセージは、*kavscanner* および *aveserver* コンポーネントによってのみ生成されます。

ファイルスキャンに関するレポートの形式は、オブジェクト形式(シンプルまたはコンテナ)によって異なります。
シンプルオブジェクトの場合、スキャンに関するメッセージは、以下のような形式になります。

- 長いメッセージ(**ShowObjectResultOnly=no**):

  "file_name" result [virus_name]

- 短いメッセージ(**ShowObjectResultOnly=yes**):

  "file_name" result

  各コマンドおよびパラメータの意味は以下の通りです。

  virus_name は、イベントが CURED、INFECTED、CUREFAILED、WARNING、および SUSPICIOUS の場合のウイルス名です。それ以外のイベントの場合、このフィールドはブランクになります。

  result – スキャンおよび駆除後にファイルに割り当てられたステータス。割り当てられる可能性があるすべてのステータスを以下の表に示します。

複合オブジェクト(アーカイブ)の場合も、長いメッセージと短いメッセージの形式があります。

- 長いメッセージ(**ShowContainerResultOnly=no**):

"archive_name"
"file_name" result [virus_name]
"file_name" result [virus_name]

- 短いメッセージ(**ShowContainerResultOnly=yes**)：

  "file_name" result

イベント/結果	意味
OK	このファイルは感染していません。
CURED（駆除モードが有効な場合のみ)	このファイルは感染していましたが、駆除に成功しました。
INFECTED	このファイルは、1 つ以上のウイルスに感染しています。駆除は要求されていません。
CUREFAILED（駆除モードが有効な場合のみ)	このファイルは、1 つ以上のウイルスに感染しています。駆除が要求されていますが、このファイルのウイルスを駆除できません。
WARNING	このファイルのコードは、既知のウイルスのコードに類似しています。
SUSPICIOUS	このファイルは、未知のウイルスに感染している疑いがあります。
ERROR	エラーが発生しているため、このファイルをチェックできません(破損したアーカイブが処理された場合など)。
PROTECTED	このファイルは暗号化されているため、チェックできません。
CORRUPTED	このファイルは破損しています。

6.7.2. コンソールに出力されるメッセージの形式

kavscanner および keepup2date コンポーネントによってメッセージがコンソールに出力されます。

コンポーネントの起動時のコマンドラインに**–q** (quiet)オプションが含まれているかどうかによって、*kavscanner* コンポーネントがコンソールに情報を出力するかどうかが決まります。このオプションが使用された場合、コンソールに情報が出力されません。*keepup2date* コンポーネントの処理に関するメッセージをコンソールに出力するには、設定ファイルで **KeepSilent=no** パラメータを設定します。

デフォルトでは、画面に表示される情報の形式および内容は、レポートファイル内の情報とまったく同じです。
kavscanner コンポーネントによってコンソールに出力される情報の内容を設定するには、設定ファイル(*kav4mailservers.conf* または代替設定ファイル)に**[display]**セクションを作成します。
このセクションでは、アーカイブ内のスキャンオブジェクトに関する情報(**ShowArchiveContent** および **ShowContainerResultOnly**)、感染していないファイルに関する情報(**ShowOK**)、およびコンポーネントの現在の処理結果に関する情報(**ShowProgress**)について、それぞれ表示するかどうかをパラメータで指定できます。
[display]セクションを作成した場合は、コマンドラインで**–x<option>**オプションを使用することにより、スキャンレポートの詳細レベルを指定できます。

6.7.3. アプリケーションのウイルス統計情報

Kaspersky Anti-Virus バージョン 5.5 では、指定した期間のウイルスアクティビティに関する統計情報を、収集して表示することができます。この機能は、Webmin によって提供される Web ベースのインタフェースから利用できます。

ウイルス統計情報の自動収集を設定するには、以下の手順を実行します。

- アプリケーション設定ファイルの**[smtpscan.report]**セクションで、**AVStatistics** パラメータに以下の値を割り当てます。

  AVStatistics=
  /var/log/kav/5.5/kav4mailservers/smtpscanner.stat

- レポートファイルから統計情報を収集するスクリプトを定期的に実行します。実行するには、コマンドラインで、以下のコマンドを入力します。

  perl /usr/libexec/webmin/kavms5.5/parse_avstat.pl \
  -sd=/var/db/kav/5.5/kav4mailservers/proc_avstat\
  /var/log/kav/5.5/kav4mailservers/smtpscanner.stat

- 上記のスクリプトのみ起動してから、更新された統計情報を Webmin で確認します。

デフォルトと異なるパスに Webmin がインストールされている場合、それに応じて/usr/libexec/webmin/kavms5.5/parse_avstat.pl パスを変更してください。

6.7.4. メッセージの追加データフィールド

バージョン 5.5 では、メッセージのヘッダに補足情報を追加できます。アプリケーションのバージョン、ウイルス定義データベースの最終更新日、現在のメッセージのウイルススキャン時刻および結果に関する情報を追加できます。

メッセージのヘッダにこれらの情報を追加するには、アプリケーション設定ファイルの**[smtpscan.group:default]**セクションで、**AddXHeaders** パラメータを定義します。

ヘッダの形式：
X-Anti-Virus:<アプリケーション名およびバージョン>, bases: <ウイルス定義データベースの最終更新日(YYYYMMDD 形式)> #<ウイルス定義データベースのレコード数>, check: <スキャン日付(YYYYMMDD 形式)> <スキャン後のステータスまたは not_checked>
例：
X-Anti-Virus:Kaspersky Anti-Virus for Unix Mail Servers version 5.5/RELEASE, bases:20041101 #102746, check:20041210 clean

第7章 KASPERSKY ANTI-VIRUS のアンインストール

Kaspersky Anti-Virus をアンインストールするには、以下の要素が必要です。

- superuser 権限(**root**)。アンインストールを開始するときにこの権限がない場合は、**root** ユーザとしてログインする必要があります。
- インストールログファイル。
- Kaspersky Anti-Virus の一部としてインストールされたファイルの名前とサイズが、インストールログファイル内に指定されているものと一致すること。
- *aveserver* 処理が停止されていること。
- メールサービスが停止されていること。

使用されているパッケージマネージャに応じて、さまざまな方法でアンインストールを開始できます。ここでは、それらの方法について詳しく説明します。

.rpm パッケージを使用して Kaspersky Anti-Virus をインストールした場合は、コマンドラインで以下のコマンドを入力してアンインストールを開始します。

```
rpm -e <package_name>
```

.deb パッケージを使用して Kaspersky Anti-Virus をインストールした場合は、コマンドラインで以下のコマンドを入力してアンインストールを開始します。

```
dpkg -r <package_name>
```

.pkg パッケージを使用して Kaspersky Anti-Virus をインストールした場合は、コマンドラインで以下のコマンドを入力してアンインストールを開始します。

```
pkg-delete <package_name>
```

アプリケーションが自動的にアンインストールされます。ソフトウェアの削除が成功した場合、それ以上メッセージは表示されません。

第8章 KASPERSKY ANTI-VIRUS の動作検証

Kaspersky Anti-Virus をインストールした後、テストウイルスを使用して設定と動作が正しいか確認します。

ここではテストウイルスは eicar（開発元：European Institute for Computer テストウイルスはコンピュータに影響を与える有害コードを含んでいないので、本当のウイルスではありません。しかし、ほとんどのアンチウイルス製品でウイルスとして認識されるものです。

アンチウイルス製品の動作確認のために本当のウイルスは絶対に使用しないでください。

テストウイルスは **EICAR** の公式サイト（http://www.eicar.org/anti_virus_test_file.htm）にて入手可能です。 インターネットに接続できない環境の場合は、次の文字列をテキストファイルで作成し、テストウイルスを作成する必要があります。

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

ファイル名は **eicar.com** としてください。

Kaspersky Anti-Virus はこのファイルを**感染した**ファイルとして検知することができ、設定に従ってファイルを処理します。
他の検知タイプを試したい場合は、下表（テスト用"ウイルス"の亜種）に従い、上記の文字列に接頭辞文字列を付与してください。

テスト用"ウイルス"の亜種

接頭辞	オブジェクトの種類
接頭辞無し標準"ウイルス"	**感染オブジェクト**。駆除できないので、オブジェクトを削除します。
CORR–	**破損オブジェクト**
SUSP–	**疑わしいオブジェクト**(未知のウイルス)

接頭辞	オブジェクトの種類
WARN–	**疑わしいオブジェクト**(既知ウイルスの亜種)
ERRO–	**スキャンエラー**
CURE–	**感染オブジェクト。**オブジェクトは駆除され、"ウイルス"のボディが CURE に変更されます。
DELE–	**感染オブジェクト。**オブジェクトは自動で削除されます。

表の左列には"ウイルス"の文字列に追加する接頭辞が表記されています例：
DELE–X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
接頭辞を追加したら、eicar_dele.com といった具合にファイル名を変更して保存します。
右列には亜種としてプログラムに検知されるオブジェクトの種類が表記されています。オブジェクトに対する処理はプログラムの設定により異なります。

第9章 よくある質問（FAQ）

インストールや設定、操作に関するFAQです。分からないことがあったら、まずこちらを参照してください。

質問：カスペルスキーアンチウイルスと他のアンチウイルスソフトを併用することは可能ですか？

プログラム間の競合を避けるため、カスペルスキーをインストールする前には他のアンチウイルスソフトを削除してください。

質問： 以前スキャンしたファイルを再スキャンしません。

プログラムは最終スキャン時から変更されていないファイルの再スキャンを行いません。NTFS 代替データストリーム上のファイルチェックサムストレージとファイルチェックサムデータベースを利用するプログラムである iChecker と iStreams テクノロジーの導入でこの機能を実現しています。

質問：コンピュータの処理能力が下がり、CPU への負荷が高いようですが？

ウイルス検出は、構造の分析やチェックサム計算、数式データの変換等を要する算出作業なため、演算処理を行うプロセッサーに負荷がかかります。またウイルス定義データベースが更新されることにより、スキャンにかかる時間が長くなることがあります。

スキャン時間を短縮するために検出が困難なウイルスやごくまれなウイルス(地域限定のウイルスなど)、スキャンが困難なフォーマット(PDF 等)などをウイルス定義データベースから省いた他のアンチウイルスソフトと異なり、カスペルスキーはコンピュータの安全を最優先に考えています。

パワーユーザ向けにスキャン対象となるファイル形式を絞ってスキャン時間を短縮できるオプションが準備されていますが、コンピュータを危険にさらす確率が高まります。プログラムは 700 種以上の圧縮ファイルに対応しています。いずれの形式も悪意あるコードを含ませることが可能なため、安全上とても大切な機能です。また 1 日約 30 とい

う勢いで新型ウイルスが誕生し、データベースは膨張し続けていますが、最新バージョンでは iChecker と iStreams･技術の開発により、旧バージョンよりも処理スピードが向上し、対応ファイル形式も増えています。

質問： ライセンスキー無しで製品を試用することは可能ですか？

ライセンスキー無しではプログラムは動作しません。

プログラムの試用をお望みの場合は 2 週間(または 1 ヶ月)有効のトライアル用キーを発行いたします。試用期間が過ぎるとライセンスキーは無効になります。

質問： ライセンスキーの期限が切れるとどうなりますか？

ライセンスキーの有効期限が切れてもプログラムは機能を続けます。アップデート機能だけが無効となるので、既にダウンロード済みの定義ファイルを利用してオブジェクトのスキャンやウイルスの駆除を実行できますが、最新のウイルスには対応できません。

ライセンス期限が切れた場合には管理者に知らせるか、販売元あるいはカスペルスキーラブスで新しいキーを購入してください。

質問： プログラムが動作しません。どうしたらいいですか？

取扱説明書あるいは弊社サイトに対応策が書かれていないか確認してください。

解決しない場合は、販売元または弊社サポートサービス(support@kaspersky.co.jp)あるいはライセンスキー情報に記載されている宛先に問い合わせてください。

メールにてお問合わせの際には、対応を早めるため、次の情報をご記入ください(メールはテキスト形式で作成してください)：

1. 件名にお使いの OS、カスペルスキー製品の名称、トラブル概要をご記入ください。例：
   Linux, カスペルスキーアンチウイルス 5.5 for Linux Mail Servers, アップデートが機能しない
2. メールはテキスト形式で作成してください。

3. 本文の始めに OS と製品のバージョン、ライセンスキーナンバーを記入してください。
4. 続けてトラブル内容をなるべく詳しく記入してください。サポート担当者は問題を完全に理解し再現を行った後にサポート連絡を行います。
5. 次のファイルを 1 つの書庫に圧縮して添付してください：
   - メール配送ソフト(MTA)の全設定
   - /etc/kav 配下の全ファイル
   - メールシステムレポートファイル
   - アンチウイルスの log ファイル　例：*/var/log/aveserver.log*
   - **ps –ax** コマンドの出力結果
   - ライセンスキーファイル
6. 次のスペックに該当する場合はその情報も合わせてご記入ください：
   - SCSI-コントローラの使用
   - かなり古いまたは最新のプロセッサーもしくは複数のプロセッサーを使用
   - 64Mb 以下あるいは 2Gb 以上のメモリを使用
7. 一日あたりのおおよそのトラフィック総量およびハードウェア負荷がピークに達していないかどうか。

質問： なぜ毎時アップデートが必要なのですか？

ほんの数年前までウイルスはフロッピーディスクを経由して広がっていたため、アンチウイルスソフトがインストールされてさえいれば、ほとんど更新を行わなくても安全を確保することができました。しかし現在では数時間の内にウイルスが世界中に広がるため、新型ウイルスに対応するためには常にプログラムを最新の状態に保つ必要が生じています。

カスペルスキーでは毎年更新の頻度を高め、今日では 1 時間おきに定義ファイルが更新されています。

また更新ファイルにはプログラムの修正や新機能といったモジュール

も含まれるため、少なくとも 1 日に 1 回は更新の実行をお奨めします。

質問： バージョン5.0 ではアップデート機能に変更はありますか？

バージョン 5.0 ではユーザ様の要望を取り入れた機能を追加したほか、更新ファイルの作成からインストールまでのアップデートプロセスの大幅な改善が図られています。

強化されたアップデート機能：

- レジューム機能の採用。更新ファイルのダウンロードが途中で失敗してもその場所からダウンロードを続行できます。
- 累積更新ファイルのサイズを半減。累積更新ファイルには全てのウイルス定義データベースが含まれているため、通常の更新ファイルよりもサイズがかなり大きくなりますが、既存の定義ファイルを利用する新技術の導入により、累積更新ファイルサイズが軽減しました。
- ダウンロード時間の短縮。最寄りのアップデート用サーバから負荷の少ないものを自動で選出してダウンロードを実行します。
- ライセンスキーのブラックリストを導入。不正なライセンスキーを使用したアップデートを遮断することによってアップデート用サーバの負荷を軽減します。
- ローカルサーバの採用。複数のコンピュータを使用する環境では、LAN 上のサーバから更新ファイルをダウンロードできる機能を追加しました。LAN で繋がれたクライアント PC はインターネットに接続せずにアップデートを実行できます。

質問：ハッカーがウイルス定義データベースに変更を加えることは可能ですか？

全てのウイルス定義データベースは著名され、アクセス時に整合性をチェックします。著名が一致しないまたはライセンス期限よりも新しいデータベースはインストールされません。

質問：Kaspersky Anti-Virus for Unix Mail Servers が動作する Linux ディストリビューションを教えてください。

Kaspersky Anti-Virus for Unix Mail Servers バージョン 5.5 は、RedHat, Debian, SuSE で動作確認しています。

サポート対象の OS については、10 ページの 1.2 項をご参照ください。

ご利用のディストリビューションが、Kaspersky がサポートするディストリビューションと互換性があれば、問題が起きる確率は非常に低いといえます。（例えば、ASPLinux は RedHatLinux と互換性がありますので、Kaspersky の動作に問題が起きる可能性は非常に低いといえます。）

Kaspersky がサポートするディストリビューション一覧にご利用中のディストリビューションが無い場合は、ライブラリの違い等が原因となり、正確に動作しない恐れがあります。この場合は、Kaspersky のテクニカルサポートに範疇外になりますことをご了承ください。

質問：tgz や tar.gz という拡張子のファイルの展開方法を教えてください。

以下のコマンドで展開してください。

```
tar -zxvf <archive_name>
```

tar コマンドの man(1)では、更に詳しい情報を得ることができますので、ご参照ください。

質問：Kaspersky Anti-Virus for Unix Mail Servers をインストールするまでは、使用中の postfix はまったく問題なく動作していたにもかかわらず、インストール後にメール配送ができなくなり、mailog に以下のログが出るようになりました。

```
Sep 23 15:17:03 server postfix/lmtp[1678]: 8238C38987:
to=<user@server.org <mailto:user@server.org>>, relay=none,
delay=1, status=bounced (localhost: host not found)
```

次のことが原因になっている可能性があります：

- ご利用中の DNS が RFC2606 に規定されている local domain を定義していない可能性があります。RFC に従い定義してください。更に詳しい情報は次の URL をご参照ください：
  http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc2606.html
- /etc/hosts ファイルに localhost が定義されていない可能性があります。通常であれば **localhost=127.0.0.1** と定義されていま

す。

質問：Windows 用の Network Control Centre で Kaspersky Anti-Virus を制御できますか？

可能です。

なお、Webmin を利用したリモート操作機能もあります。

質問：コンソールに出力される情報をファイルに書き込むことはできますか？

次のコマンドを使用してください：

```
$ some_app > ./text_file 2>&1
```

例：

```
$keepup2date > ./updater.log 2>&1
```

上記の場合、標準出力に現れるメッセージは、updater.log にも記録されています。

付録 A. カスペルスキーラブス

1997 年の創始以来、カスペルスキーラブスは、情報セキュリティ技術界のリーダーとして知られ、コンピュータとネットワークをリスクウェアやスパム、ハッカーの攻撃等から保護する高性能かつ包括的な情報セキュリティソフトウエアを提供しています。
カスペルスキーラブスは本社ロシアを始め英、仏、独、日、米(CA)、中、ボーランド、ベネルックス 3 国に支社を構える国際企業で、世界各国 500 以上の企業とのパートナーネットワークがあります。仏にはヨーロッパアンチウイルスリサーチセンターの新部門も設立されました。
現在カスペルスキーラブスは 250 名以上の高度専門家を抱え、内 9 名が MBA を、15 名が博士号を取得し、2 名はコンピュータアンチウイルスリサーチャーズ機構(CARO)のメンバーです。
14 年余に渡るウイルス対策でスタッフが培った知識と経験がカスペルスキーラブスの最大の財産となり、ウイルスの動向をも予知し、現在はもちろん一歩先行くセキュリティ製品とサービスを提供し続けています。
世界最高水準を自負する弊社の主力ウイルス対策製品はワークステーションを始めファイルサーバやメールサーバ、ファイアウォール、ポケット PC をウイルスの驚異から守ります。また柔軟な管理ツールを備えることにより、企業のネットワークにも万全なセキュリティを提供します。また Nokia ICG(米)や F-Secure(フィンランド)、Aladdin(イスラエル)、Sybari(米)、G Data(独)、Deerfield (米)、Alt-N(米)、Microworld(印)、BorderWare(加)などでカスペルスキーラブスのアンチウイルスエンジンが採用されている事実も製品の水準を雄弁に物語っています。
クライアントは製品の安定動作はもちろん、設計から開発、サポートまで、様々な要件に応える高度サービスを享受いただけます。ウイルス対策の要となるウイルス定義データベースは毎時間更新され、24 時間多言語でのサポートを提供しています。

A.1. カスペルスキーラブスのその他の主な製品

Kaspersky® OnLine Scanner Pro
カスペルスキー®オンラインスキャナプロは Web サイトで提供される Microsoft ActiveX®テクノロジーをベースにしたファイルのスキャンサービスに、感染ファイルの駆除機能と以下の機能を付加した製品です：

- 実行形式アーカイブとメールデータベースのスキャンに対応

- スパイウェアを検知する拡張定義ファイルの採用
- スキャン結果をテキスト形式のレポートファイルに出力

Kaspersky® Security for PDA

カスペルスキー®セキュリティ for PDA は、PalmOS や WindowsCE 上で動作する PDA 向けのセキュリティソリューションです。保存データや PC、拡張カード、ROM ファイル経由のデータ及びデータベースの保護を提供します。パッケージには、次のアンチウイルスツールが含まれています：

- **アンチウイルススキャナー** - 必要に応じて PDA と拡張カードのデータをスキャンします
- **アンチウイルスモニター** - 他の携帯端末や HotSync・から転送されるファイルを監視し、ウイルスを遮断します

カスペルスキー®セキュリティ for PDA は外部からの侵入を遮断し、PDA と拡張カード上のデータを保護します。

Kaspersky Anti-Virus® Business Optimal

カスペルスキーアンチウイルス® Business Optimal は、中小企業のネットワーク向けセキュリティーパッケージです。
製品は、次の構成向けに最大級のセキュリティを提供します：

- ワークステーション - Windows 98/ME、Windows NT/2000/XP、Linux
- ファイルサーバ - Windows NT 4-0 Server、Windows 2000/2003 Server/Advanced Server、Windows 2003 Server、Novell Netware、FreeBSD、OpenBSD、Linux
- メールサーバ - Microsoft Exchange 5-5/2000/2003 、Lotus Notes/Domino、Postfix、Exim、Sendmail、Qmail
- インターネットゲートウェイ：CheckPoint Firewall ・1；MS ISA Server

製品には集中管理ツールである、カスペルスキーAdministration Kit が含まれます。使用する OS とアプリケーションに応じてアンチウイルスソフトを自由に選ぶことができます。

Kaspersky® Corporate Suite

カスペルスキー®コーポレートスイートは、あらゆる規模に対応する企業向け総

合情報セキュリティシステムです。今日企業のネットワークで採用されているほとんどの OS に対応し、統合インタフェースを持つ 1 つのコンソールで管理される本製品は、様々なネットワーク要件を満たす高制度で高品質な安全を提供します。
対応プラットフォーム：

- ワークステーション - Windows 98SE/Windows NT/2000/XP/Linux
- ファイルサーバ - Windows NT 4.0 Server、Windows 2000/2003 Server/Advanced Server、Windows 2003 Server、Novell Netware、FreeBSD、OpenBSD、Linux
- メールサーバ - Microsoft Exchange 5.5/2000/2003、Lotus Notes/Domino、Postfix、Exim、Sendmail、Qmail
- インターネットゲートウェイ：CheckPoint Firewall ・1；MS ISA Server
  - PDA - Windows CE、Palm OS

製品には集中管理ツールである、カスペルスキーAdministration Kit が含まれます。使用する OS とアプリケーションに応じてアンチウイルスソフトを自由に選ぶことができます。

Kaspersky® Anti-Spam

カスペルスキー®アンチスパムは、革新的な言語解析テクノロジーと最新鋭のメール(RBL リストと公式文書を含む)フィルタリングを結合した中小企業向けのスパム対策ソフトウェアです。不要なトラフィックの 95％を識別、カットすることが可能です。
ネットワークの入り口に導入することにより、受信メールを監視してスパムと認識されるオブジェクトを遮断できます。あらゆるメールシステムをサポートするので、既存のメールサーバや専用サーバをそのまま使用できます。
高度なスパムメールの認識精度は、カスペルスキーラブスの言語研究所によって日々更新されるフィルタリングデータベースによって実現されています。

A.2. お問い合わせ

ご意見・ご質問等はカスペルスキーラブスまたは弊社ディストリビュータにてお伺いしております。

WWW：	http：//www.kaspersky.co.jp http：//www.viruslistjp.com

E-mail	support@kaspersky.co.jp

付録 B. 使用許諾契約書

Kaspersky Labs Japan ソフトウェア使用許諾契約書

株式会社 Kaspersky Labs Japan(以下カスペルスキーラブス)本プログラムをご使用になる前に、以下の文章をよくお読みください。
この度は、弊社製品をご利用いただき、まことにありがとうございます。弊社では製品につきまして、下記のソフトウェア使用許諾契約書を設けさせていただいており、お客様が下記契約書にご同意いただいた場合のみ製品をご使用いただいております。

第１条（定義）

1. 「本プログラム」とは、本契約に基づき提供されるカスペルスキーアンチウィルス及び関連資料を指します。
2. 「クライアント機器」とは本プログラムをインストールするコンピュータあるいはワークステーション、個人デジタル機器およびその他電子機器を指します。

第２条（許諾事項）

１．本プログラムにはライセンスキー（識別キーファイル）が付属しています。本契約の条項に同意されたお客様に対し、カスペルスキーラブスは、本契約の有効期間中、本プログラムの非独占的かつ譲渡不可の使用権を許諾します。お客様は本プログラムを 1 台のクライアント機器にのみインストールすることができます。
２．本プログラムは、単独のソフトウェア・プログラムとしてライセンスされ、同時に２台以上のクライアント機器や２人以上のユーザーが利用することは出来ません。
３．製品は、クライアント機器のメインメモリにロードする、もしくはストレージ（ハードディスク、CD-ROM、その他の記憶装置）にインストールした場合、そのクライアント機器上で「使用中」となります。
４．お客様はバックアップの目的で本プログラムのコピーを一部のみ制作することが出来ますが、当該コピーについては、不法コピーや不正利用防止のために適切な措置を講ずるものとします。
５．お客様が、本プログラムのインストールされたクライアント機器を売却あるいは処分される場合は、本プログラムがあらかじめ削除されていることを確認してください。

第３条（禁止事項）

１．　本プログラムの全部または一部を複製、改変、リバースエンジニアリング、翻案、再配布、譲渡、貸与、再使用許諾、中古取引、レンタル、リースすることはできません。

２．お客様は本プログラムの逆コンパイル、リバースエンジニアリング、逆アセンブル、その他の方法で本プログラムの全部または一部を可読可能な形式に変換したり、第三者にそれらの行為を許可したりする事は出来ません。

３．本プログラムに付されているカスペルスキーの商標、ロゴおよび画面イメージをカスペルスキーラブスの事前の書面による許諾なく使用し本プログラムの一部または全部を配布することはできません。

４．お客様は、製品の貸与およびリース、またライセンス権利の譲渡、サブライセンスの発行を行うことはできません。

５．お客様は、この製品をウイルス符号、ウイルス検知ルーチン、悪意のあるコードやデータ検知のための他のデータやコードの生成を意図した自動、半自動、手動ツールとして、使用できません。

第４条　(サーバモード)

1.　適用可能な価格表もしくは当該の製品個々に適用される製品パッケージで、使用が許可されている場合に限り、クライアント機器上、または複数ユーザー間あるいはネットワーク環境（以下「サーバモード」という）のサーバ上で製品をご利用いただくことができます。クライアント機器や「シート」が同時接続しているかどうか、あるいは実際にその製品を使っているかどうかにかかわらず、それらのクライアント機器やサーバに接続する「シート」毎に、相当量のライセンスが必要となります。製品に直接アクセスする、あるいは利用することにより、クライアント機器やシートの数を減らすような製品、またはハードウェア（「マルチプレクシング」や「プーリング」などの製品やハードウェア）を使用しても、必要なライセンス数を減らすことは出来ません。製品に接続可能なクライアント機器やシートの数は、ユーザーが取得したライセンス数を上回ってもかまいませんが、その場合、お客様は実際に使用される製品数が、取得されたライセンス数を上回らないための、適当な予防措置を講じるものとします。合法的な使用に限り、このライセンスによって、ユーザーは製品所有通知を含むことを条件に、クライアント機器および/またはシートむけに製品のダウンロード複製の権利が与えられます。

第５条　(ライセンス)

1.　本契約は以下の条件によって契約が終了する場合を除き、１年間が有効期間となります。ここに記載された条件、制限、要件に反する行為が

お客様により行われた場合、契約は自動的に解除されます。本契約の解除および有効期間切れの場合、お客様が保有している本製品及びそのコンポーネントを全て破棄してください。お客様が、製品および資料のコピーを破棄した時点で、本契約は終了します。

製品が、製品購入契約書やパッケージにおいて使用可能な製品が指定され、ライセンスボリューム条項が適用されている場合、お客様はボリュームライセンスで指定された数のクライアント機器に、コピーやインストール、利用が行えます。

2. お客様は、ライセンス数以上の製品がクライアント機器にインストールされないことを保証するための、適切な予防措置を講じるものとします。また、資料に関しては、合法利用の範囲内で、著作権情報を含むことを条件に、ライセンス数内でダウンロード及びコピーが許諾されます。

第 6 条 (サポート)

1. カスペルスキーラブスは、次の条件を満たすお客様に、下記のサポートサービスをライセンスの有効期間に渡り提供します。
   1.1. 当該サポートサービスを含む製品への支払い
   1.2. この契約書あるいはカスペルスキーラブスの Web サイトにあるサポートサービス登録（書）に、この契約書とともにカスペルスキーラブスから提供される「ライセンスキー」情報を記載して、適切にサービス登録が行われた場合。お客様がサポートサービスの提供条件を満たしているか否かはカスペルスキーの判断によるものとします。
2. 契約の満了時にサポート料金をお支払いいただき、サポートサービスの再登録を行って、年間契約を更新されない限り、契約は更新されません。
3. サポートサービスの登録を行うことにより、お客様はこの契約書に付属しているカスペルスキーラブスのプライバシーポリシーの条項に同意するとともに、プライバシーポリシーに詳述されているとおり、他国へのデータの転送を明示的に同意したものとみなされます。
4. サポートサービスとは
   1.1. アンチウイルス・データベースを毎週更新
   1.2. バージョン・アップを含む無料製品更新
   1.3. 販売元による電子メール及び電話にての拡張技術サポート

第 7 条 (著作権)

本ソフトウェアは日本の著作権法並びに国際条約の規定、その他使用される国において適用される法律により保護されています。カスペルスキーラブスならびに開発元は、は本ソフトウェアの一切の権利、権原および持分につき、本ソフトウェアに含まれるすべての著作権、特許、商標、営業秘密その他の知的財

産権を所有し、維持しています。お客様は、本ソフトウェアの所有、インストール、または使用など知的財産権に関する権利がお客様に譲渡されるものではないことを了承します。お客様はさらに、本契約に明示的に規定されていない限り、本ソフトウェアのいかなる権利もお客様が取得するものではないことを了承します。お客様は、本ソフトウェア及びマニュアルの全ての複製物に、本ソフトウェアに表示されるものと同じ財産権が表示されることに同意します。

第 8 条　(機密保持)
お客様は、特定のデザインと個々のプログラム構造およびライセンスキーを含む製品と資料が、カスペルスキーラブスが所有権をもつ機密情報によって構成されていることに同意したとみなされます。お客様は、事前にカスペルスキーラブスの文書による承認なしに、公開、提供、あるいはそれらの機密情報を第三者が使用可能な形式にしてはいけません。お客様は、このような機密情報を守るために適切なセキュリティ手段を講ずる必要がある他、ライセンスキー情報の機密を保持する義務を持ちます。

第 9 条（保証）

1．　本プログラムはお客様に現状有姿にて提供され、カスペルスキーラブスは、本プログラムに対するバグや不具合を是正する責任を有さないものとします。
2．　カスペルスキーラブスは、本プログラムがお客様の特定の目的に適合すること、中断または誤りなく動作すること、第三者の権利を侵害していないことおよび本プログラムにバグや不具合がないことを保証しません。
3．　カスペルスキーラブスは、本プログラムによるあらゆる既知のウイルスの識別、および未感染ウイルスを誤って報告しない、ということについて、何等の保証も行いません。
4．　カスペルスキーラブスは、初回インストールから 90 日間は、通常の使用下において、マニュアルに則った方法での使用に瑕疵がないことを条件に、その公表された性能を保証します。
5．　お客様の唯一の救済および(i)の保証の違反に対するカスペルスキーラブスの全責任は、カスペルスキーラブスが決定し、保障期間にカスペルスキーラブスあるいはカスペルスキーラブスの正規販売代理店に報告あるいは指定された場合、製品の修理、交換、返金がなされます。
6．　以下のいずれかの条件に該当する場合、(1)の保証は適用されません。
(a) 使用者がカスペルスキーラブスの許可なく本製品を改竄した場合。
(b) 想定外の方法で本製品を使用した場合。
(c) 本契約書で許可された範囲を超えて使用した場合、

7． 本契約書にて述べられた保証および条件は、(E)で定義する条件の上で、本製品および付属書類の供給、供給内容、供給の不備、供給の遅れに関し、保証するものとする。但し、本契約書が本製品及び資料を取得する国の法律及び慣習と異なる場合は別途協議するものとする(この保証は、契約者が満足するまでの間無制限に行うものではなく、契約者が本製品を使用するにあたって一般的に必要と考えられる知識、及び技術を持ち合わせていることが前提であり、また一般常識内で保証するものとする)。

第 10 条 (免責)

1. 本契約のいかなる規定も下記の責任に対しカスペルスキーラブスの免責を除外または制限するものではありません：

(a)虚偽の不法行為
(b)注意義務違反による不履行、契約条項の不履行によって発生した死亡または身体障害
(c) 法による除外が不可能な義務

2. (1)の条件の下、次の損害または被害に対し、開発者は（契約、不法行為、賠償にかかわらず）いかなる責任も（そのような損失や被害を予見した、予見できた、知りえたかにかかわらず）負担することはありません。

(a) 収益の損失
(b) 実および予想利益(契約における利益の損失を含む)の損失;
(c) 金銭利用の損失
(d) 予想された貯蓄の損失
(e) ビジネス損失
(f) 機会損失
(g) 善意の損失
(h) 評判の損失
(i) データ被害あるいは改悪による損失
(j) 間接又は派生的滅失毀損（疑惑回避のため(ii)項のタイプによる滅失毀損を含む）

3. (1)の条件のもと、（契約、不法行為、賠償にかかわらず）製品の提供に関連して、カスペルスキーラブスが本ソフトウェアのライセンスに対して設定した表示価格を超える金額において、損害に対して責任を負担することはありません。

第 11 条 (プライバシー)

本契約を締結することにより、お客様は、カスペルスキーラブスがお客様の名前、住所、メール・アドレスおよびクレジットカードの情報を含め、お客様に関する個人情報を収集し、保有することができることに同意することになります。お客様の個人情報は、主としてサービスや製品の機能をお客様に提供するために使用されます。カスペルスキーラブスは、またお客様の個人情報を使用してお客様と付加的なやり取りを行う場合がありますが、カスペルスキーラブスからこのような通信を受け取るかどうかはお客様自身が決定することができ、適切な法の規定の下に行われます。カスペルスキーラブスは他の企業または個人（「下請業者」）を雇用して当社に代わって業務を行なわせることがあります。その例として、支払いの処理、注文の履行、マーケティング支援の提供、ならびに顧客サービスの提供が含まれます。カスペルスキーラブスは、かかる業務を行なう下請業者が業務を果たすためにお客様の個人情報を共有しますが、他の目的のために使用することはありません。本契約を締結することにより、お客様は、上述した目的のためにお客様の個人情報をカスペルスキーラブス本社に転送することができることに同意することになります。お客様は、お客様の個人情報を当社がどのように収集、使用および転送するか、および前述したやり取りの停止あるいは登録解除方法の詳細をカスペルスキーラブス Web サイト (www.kaspersky.co.jp)のカスペルスキーラブスプライバシーポリシーを参照できます。

第 12 条　(その他)　この契約の実行と解釈は日本の法に準拠します。カスペルスキーラブスが申請者として日本の管轄裁判所に手続きを申請した場合、当事者は何れの主官裁判所においても手続きを開始することが出来ます。

株式会社 Kaspersky Labs Japan